Electronic Design®

THE AUTHORITY ON
EMERGING TECHNOLOGIES
FOR DESIGN SOLUTIONS

DECEMBER 2017 electronicdesign.com

TAKING ON ELECTRONIC WASTE

Could recycling be a new revenue stream and an environmental boon? p33

$10.00

360° Innovation
COVERAGE
SAME-DAY SHIPPING
On orders entered by 8:00 pm CENTRAL
NEXT-DAY DELIVERY
1.800.344.4539
DIGIKEY.COM
Digi-Key ELECTRONICS
6 MILLION+ PRODUCTS ONLINE | 650+ INDUSTRY-LEADING SUPPLIERS | 100% AUTHORIZED DISTRIBUTOR
Digi-Key is an authorized distributor for all supplier partners. New products added daily. Digi-Key and Digi-Key Electronics are registered trademarks of Digi-Key Electronics in the U.S. and other countries. © 2017 Digi-Key Electronics, 701 Brooks Ave. South, Thief River Falls, MN 56701, USA
ecia MEMBER
ecsn member
CEDA

December 2017 VOLUME 65, ISSUE 12

IN THIS ISSUE

FEATURES

12

17

33

COLUMNS & DEPARTMENTS

IDEAS FOR DESIGN

45

EDITORIAL MISSION:
To provide the most current, accurate, and in-depth technical coverage of the key emerging technologies that engineers need to design tomorrow's products today.

ELECTRONIC DESIGN (ISSN 0013-4872) is published monthly by Penton Media Inc., 9800 Metcalf Ave., Overland Park, KS 66212-2216. Paid rates for a one-year subscription are as follows: $120 U.S., $180 Canada, $240 International. Periodicals postage paid at Kansas City, MO, and additional mailing offices. Editorial and advertising addresses: ELECTRONIC DESIGN, 1166 Avenue of the Americas, New York, NY 10036. Telephone (212) 204-4200. Printed in U.S.A. Title registered in U.S. Patent Office. For subscriber services or to order single copies, write to Electronic Design, PO Box 2100, Skokie, IL 60076. POSTMASTER: Send change of address to Electronic Design, PO Box 2100, Skokie, IL 60076. Canadian Post Publications Mail agreement No. 40612608. Canada return address: IMEX Global Solutions, P.O. Box 25542, London, ON N6C 6B2.

ON ELECTRONICDESIGN.COM

Will A.I. Become Your Co-Pilot on the Road?

Artificial intelligence will be used to augment the driver's ability to control the car under different operating conditions. The amount of AI software and hardware required, though, will far surpass any computer system in today's vehicles.

http://www.electronicdesign.com/automotive/will-artificial-intelligence-become-your-co-pilot-road

A Hybrid Approach to Energy Storage

Although it is common to find supercapacitors in many power-electronics devices, hybrid energy storage technology could increase the commercial adoption of supercapacitors in grid-scale solutions.

http://www.electronicdesign.com/power/hybrid-approach-energy-storage

What Can You Make With Ada?

Check out Ada and SPARK if you really want to write safe, reliable, and secure software while concentrating on the application, rather than not accidentally adding bugs. They will still wind up in applications, but more likely in the algorithm rather than the implementation.

http://www.electronicdesign.com/embedded-revolution/what-can-you-make-ada

Passive vs. Active Noise Cancellation

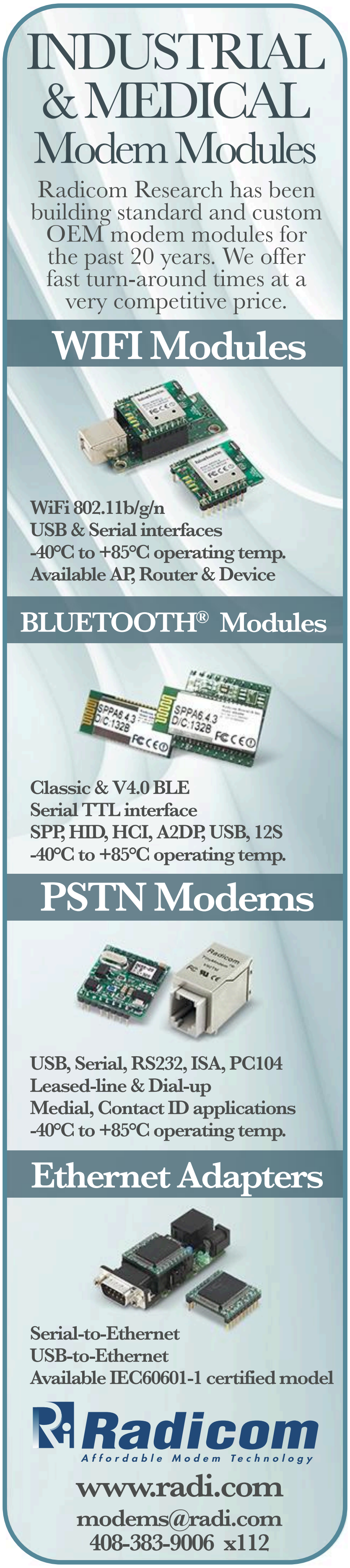
Increased use of smartphones and other devices for music playback gives more weight to features like noise cancellation. So how can system developers determine the best noise-cancellation option to differentiate their products and still appeal to discerning consumers?

http://www.electronicdesign.com/industrial-automation/what-s-difference-between-passive-and-active-noise-cancellation

ElectronicDesign®

FOLLOW US ON FACEBOOK AND TWITTER

(ElectronicDesign) (@ElectronicDesgn)



ElectronicDesign. **DECEMBER 2017**

EDITORIAL

CONTENT DIRECTOR: **NANCY K. FRIEDRICH** nancy.friedrich@penton.com
CONTENT PRODUCTION DIRECTOR: **MICHAEL BROWNE** michael.browne@penton.com
CONTENT PRODUCTION SPECIALIST: **ROGER ENGELKE** roger.engelke@penton.com
PRODUCTION EDITOR: **JEREMY COHEN** jeremy.cohen@penton.com
EMBEDDED/SYSTEMS/SOFTWARE: **WILLIAM WONG** bill.wong@penton.com
ANALOG/POWER: **MARIA GUERRA** maria.guerra@penton.com
CONTENT OPTIMIZATION SPECIALIST: **WES SHOCKLEY** wes.shockley@penton.com
ASSOCIATE CONTENT PRODUCER: **LEAH SCULLY** leah.scully@penton.com
ASSOCIATE CONTENT PRODUCER: **JAMES MORRA** james.morra@penton.com
CONTRIBUTING EDITOR: **LOUIS E. FRENZEL** lou.frenzel@penton.com

ART DEPARTMENT

GROUP DESIGN DIRECTOR: **ANTHONY VITOLO** tony.vitolo@penton.com
SENIOR ARTIST: **JIM MILLER** jim.miller@penton.com
CONTENT DESIGN SPECIALIST: **JOCELYN HARTZOG** jocelyn.hartzog@penton.com
CONTENT & DESIGN PRODUCTION MANAGER: **JULIE JANTZER-WARD** julie.jantzer-ward@penton.com

PRODUCTION

GROUP PRODUCTION MANAGER: **CAREY SWEETEN** carey.sweeten@penton.com
PRODUCTION MANAGER: **FRAN VAUGHN** fran.vaughn@penton.com

AUDIENCE MARKETING

USER MARKETING DIRECTOR: **BRENDA ROODE** brenda.roode@penton.com
USER MARKETING MANAGER: **DEBBIE BRADY** debbie.brady@penton.com
FREE SUBSCRIPTION/STATUS OF SUBSCRIPTION/ADDRESS CHANGE/MISSING BACK ISSUES
OMEDA **T** | 847.513.6022 **TOLL FREE** | 866.505.7173

SALES & MARKETING

MANAGING DIRECTOR: **TRACY SMITH** **T** | 913.967.1324 **F** | 913.514.6881 tracy.smith@penton.com

REGIONAL SALES REPRESENTATIVES:

AZ, NM, TX: **GREGORY MONTGOMERY** **T** | 480.254.5540 gregory.montgomery@penton.com

AL, AR, SOUTHERN CA, CO, FL, GA, HI, IA, ID, IL, IN, KS, KY, LA, MI, MN, MO, MS, MT, NC, ND, NE, NV, OH, OK, SC, SD, TN, UT, VA, WI, WV, WY, CENTRAL CANADA: **JAMIE ALLEN** **T** | 415.608.1959 **F** | 913.514.3667 jamie.allen@penton.com

CT, DE, MA, MD, ME, NH, NJ, NY, PA, RI, VT, EASTERN CANADA:
SHANNON ALO-MENDOSA **T** | 978.501.9116 shannon.alo-mendosa@penton.com

AK, NORTHERN CA, OR, WA, WESTERN CANADA: **STUART BOWEN** **T** | 425.681.4395 stuart.bowen@penton.com

INTERNATIONAL SALES:
GERMANY, AUSTRIA, SWITZERLAND: **CHRISTIAN HOELSCHER** **T** | 011.49.89.95002778
christian.hoelscher@husonmedia.com

BELGIUM, NETHERLANDS, LUXEMBURG, UNITED KINGDOM, SCANDINAVIA, FRANCE, SPAIN, PORTUGAL:
JAMES RHOADES-BROWN **T** | +011 44 1932 564999 **M** | +011 44 1932 564998 james.rhoadesbrown@husonmedia.com

ITALY: **DIEGO CASIRAGHI** diego@casiraghi-adv.com

PAN-ASIA: **HELEN LAI** **T** | 886 2-2727 7799 helen@twoway-com.com

PAN-ASIA: **CHARLES LIU** **T** | 886 2-2727 7799 liu@twoway-com.com

PLEASE SEND INSERTION ORDERS TO: orders@penton.com

PENTON REPRINTS: **WRIGHT'S MEDIA** **T** | 877.652.5295 penton@wrightsmedia.com

LIST RENTALS/
SMARTREACH CLIENT SERVICES MANAGER: **JAMES ADDISON** **T** | 212.204.4318 james.addison@penton.com

ONLINE

PRODUCT DEVELOPMENT DIRECTOR **RYAN MALEC** ryan.malec@penton.com

DESIGN ENGINEERING & SOURCING GROUP

EXECUTIVE DIRECTOR OF CONTENT AND USER ENGAGEMENT: **NANCY K. FRIEDRICH**
GROUP DIRECTOR OF OPERATIONS: **CHRISTINA CAVANO**
GROUP DIRECTOR OF MARKETING: **JANE COOPER**

PENTON

1166 AVENUE OF THE AMERICAS, 10TH FLOOR
NEW YORK, NY 10036 **T** | 212.204.4200

Electronic Design | Machine Design | Microwaves & RF | Source ESB | Hydraulics & Pneumatics |
Global Purchasing | Distribution Resource | Power Electronics | Defense Electronics

PENTON IS AN INFORMA BUSINESS

NANCY FRIEDRICH | Director of Editorial Content
nancy.friedrich@penton.com

Fisker's Rise, Fall —and Rise?

Once hailed as a game-changing EV automaker, the carmaker is reborn under its original founder and making remarkable claims around solid-state battery technology.

Fisker Inc.'s Emotion heralds a breakthrough in graphene battery power.

It's been quite a while since Tesla wasn't the biggest name in electric vehicles (EVs). But if you think back over the last decade or so, you may recall the Fisker Automotive debacle. This EV firm, launched by Henrik Fisker and Bernard Koehler, created the Karma EV (now the Karma Revero, as what was left of Fisker became Chinese-owned luxury carmaker Karma Automotive). In doing so, it massively hemorrhaged money, laid off much of its staff, suffered employee lawsuits, and defaulted on and lost much of a U.S. Department of Energy loan of almost $530 million. Although Fisker Automotive succeeded in only building some 2,000-odd vehicles, they were largely heralded to be beautiful and exceptionally designed. In fact, Tesla attempted to sue Fisker, saying the company had copied some of its designs. Tesla lost, but Fisker disappeared anyway—until now. The car brand has been reborn as Fisker Inc. and, with the Consumer Electronics Show (CES) approaching in January, is again making headlines.

The key to Fisker's current claim on the spotlight is its solid-state battery innovation. The firm just patented lithium-ion batteries that it expects to mass-produce in the next five to six years. According to an article by engadget, "Fisker claims the batteries it's developing have an energy density 2.5 times that of current batteries, and they should be capable of providing a 500-mile driving range. The company also says the batteries could be recharged in as little as a minute."

As this patent announcement made headlines, however, the internet was abuzz with a mix of awed and incredulous responses to its claims. For comparison's sake, the Tesla Supercharger takes an estimated 30 minutes to recharge. Tesla's longest-range model, the S 100D, provides roughly 335 miles per charge. The EV industry is hoping for a solid-state leap, but questions remain about whether Fisker can really deliver on these patent claims in the timeline it suggests. The battery technology is scheduled to be "on display" at CES, although it's unclear if or how Fisker will actually be demonstrating its capabilities.

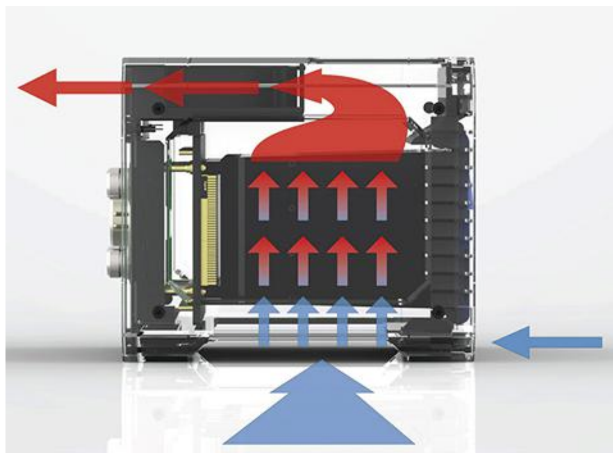
Over the summer, there were reports that the first Fisker Inc. vehicle—dubbed the EMotion—would herald a new graphene battery breakthrough. The timeline clearly didn't pan out the way the company hoped, but the website touts a 400-plus-mile range and 9-minute charging to 125 miles with lithium-ion. The price starts at $129,900 for this luxury car, which won't be available until 2019. If the firm can turn a profit and make its battery claims into viable solutions, however, it will propel the EV and potentially many other industries ahead in a revolutionary rather than evolutionary leap.

News

VITA 48.8 AIR-FLOW COOLING Almost Doubles Avionics Payload

Reducing size, weight, and power (SWaP) always tops the designer's checklist when it comes to rugged defense and airborne systems. Nowhere is it more paramount than with smaller airborne systems like drones. Heavy conduction-cooled systems provide the performance needed for these applications, but the added weight and cost can make some solutions impractical. Another approach was needed so that hotter, higher-performance commercial-off-the-shelf (COTS) systems could operate without weighing down the overall device.

The ANSI Standard ANSI/VITA 48.8-2017, "Mechanical Standard for Electronic VPX Plug-in Modules Using Air Flow Through Cooling," is a bit long-winded, but it's essentially an air-cooled standard *(Fig. 1)*. It delivers cooling performance comparable to conduction-cooled systems, yet is easier to implement and weighs much less than a comparable conduction-cooled system. Systems that employ VITA 48.8 can nearly double the amount of VPX modules in the system.

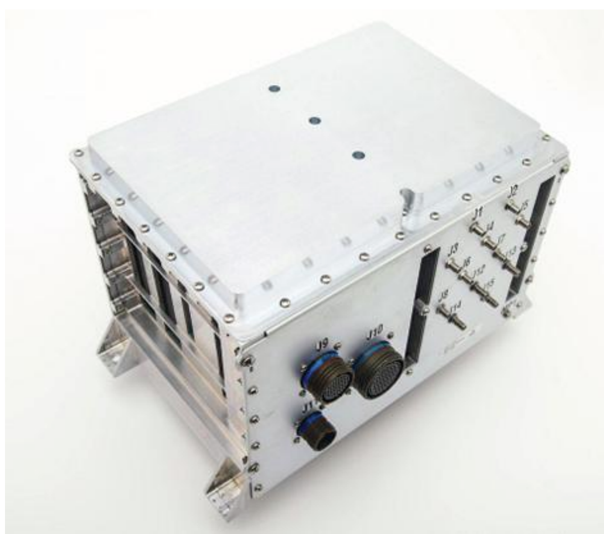


1. The VITA 48.8 standard defines the board positioning that allows air flow between boards, leading to increased cooling capability without using more expensive and heavy conduction-cooled solutions.

The VITA 48.8 Working Group was sponsored by Lockheed Martin, Curtiss-Wright, and Abaco, and chaired by Curtiss-Wright. The standard will be initially applied to fixed-wing and rotary-wing aircraft electronics. The standard addresses COTS 3U and 6U VPX form factors with power densities as high as 200 W/cm^2, allowing designers to take advantage of the latest processors and GPUs.

"Embedded system customers will benefit from the recent ANSI ratification of VITA 48.8," says Lynn Bamford, Curtiss Wright Senior Vice President and General Manager, Defense Solutions division. "As a formal open architecture standard, VITA 48.8 delivers advanced air-flow-through cooling while delivering a great combination of weight and cost savings ideal for use in space-, weight-, and power-constrained aircraft such as rotorcraft and UAV platforms. COTS 3U and 6U VPX solutions are now being deployed with power densities as high as 200 W per square centimeter, resulting from the latest processors. VITA 48.8 provides a low-cost, effective means to cool the latest generation of components."

A number of demonstration systems have already been created. For example, Lockheed Martin developed a 25-lb., hybrid conduction system based on VITA 48.8 *(Fig. 2)*.



2. Lockheed Martin's 25-lb. hybrid conduction and VITA 48.8 air-flow-through box provides the same functionality as a 40-lb. conduction-cooled system.

The system uses VITA 48.8 an air-flow-through box that provides the same functionality as a 40-lb. conduction-cooled system. This system was integrated into the S-97 Raider attack helicopter platform that can fly as high as 10,000 feet and reach speeds of over 200 knots.

VITA 48.8 helps reduce weight and cost in a number of ways. The 3U and 6U modules are still sealed from the environment with metal plates on both sides, where the airflow occurs. This approach eliminates the use of wedgelocks and ejector/injector handles normally found on conduction-cooled systems. VITA 48.8 also supports alternative air-flow arrangements that allow for an air inlet at both card edges.

Conduction-cooled systems require a heavy metal frame. With VITA 48.8 systems, however, different materials can be used for the frame. This led to Curtiss-Wright's development of a 3D-printed plastic case *(Fig. 3)*. Developers will have more options in creating cases, including how air flow will work within the system.

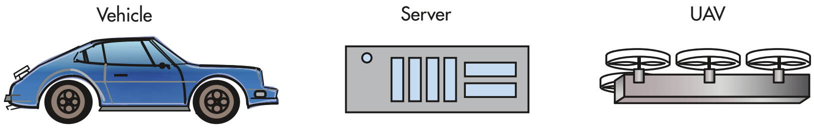
It appears VITA 48.8 is destined to have a significant impact on the rugged embedded space, particularly in terms of defense and avionic applications. ■

WILLIAM WONG, Technology Editor

3. A VITA 48.8 frame no longer has to act as a conduction-cooling system. Thus, it can be made out of lighter materials such as this Curtiss-Wright 3D-printed plastic case.

AMAZON'S LATEST PATENT: Drones that Charge Vehicles

THROUGH THE USE of example systems, devices, and methods, Amazon's newest patent describes a method to deliver energy using an uncrewed autonomous vehicle (UAV). The patent is intended for vehicles drawing energy from spinning flywheels, combusting hydrocarbons, drawing electric current from capacitors, and so forth. According to the patent, the vehicle could be configured to transport people or items. The system in the patent comprises three parts: a vehicle, a UAV, and a server *(Fig. 1).* But it could include multiple vehicles, UAVs, and servers.



1. A server may select a UAV and provide instructions to transfer energy to a rechargeable battery at a rendezvous location. *(Courtesy of freepatentsonline.com)*

THE VEHICLE

Beyond electric vehicles, the patent notes that the vehicle could include various forms of transportation including cars, trucks, bicycles, etc. The patent also mentions that the vehicle could be controlled by an operator or could operate semiautonomously or fully autonomously. In addition, the vehicle could include an energy source and a power-management module—referred to as the "energy source management module"—to monitor the amount of energy available from the energy source. As a result, it could determine whether there is a need for the vehicle to receive energy. This module also could be configured to monitor the amount of energy that is delivered to the vehicle during energy transfer.

The energy source may comprise one or more devices that provide energy so that vehicle processes may be performed utilizing electric, chemical, or mechanical devices. Those devices store energy for vehicle operation. An example could be rechargeable batteries that supply electric energy. The patent specifically talks about delivering gasoline with a vehicle containing a docking mechanism to transfer fuel from a UAV to a vehicle using fuel transfer connectors. The vehicle in the example could also generate environmental data that indicates, for example, the presence of a tree or another object or hazard. This data could be transferred to the UAV and used when docking with a vehicle *(Fig. 2)*.

THE UAV

The uncrewed autonomous vehicle is described as a mobile machine with no human operator aboard who can operate in one or more autonomous or semiautonomous modes. It could be configured to manage route selections, navigation, piloting, etc. Amazon's patent mentions how the UAV could have limited altitude (1.86 miles) and range (34.2 miles) compared to human-crewed aircraft. It could also weigh less than 99 lb.

In the patent, it is interesting to see that they are also describing Amazon prime air delivery service *(Fig. 3)* when they say, "The UAV could be owned by or associated with merchants, customers, or commercial couriers. For example, a merchant could use the UAV to deliver items that are ordered by the customer."

The UAV could use various authentication processes for protection and control to prevent or reduce energy theft. For example, the UAV could be protected from connecting with vehicles controlled

QUALCOMM REBUFFS BROADCOM'S $105 BILLION BID as Far Too Low

QUALCOMM'S BOARD LAST MONTH formally rejected Broadcom's $105 billion takeover bid, arguing that it "significantly undervalues" its business. The deal was already a long shot, facing an obstacle course of antitrust regulators and the uncertainty of Qualcomm's deal for NXP Semiconductors.

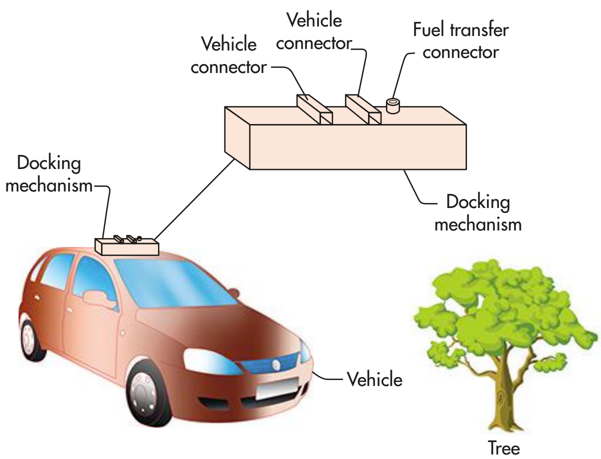
The company said that its board voted unanimously to reject the $70 per share bid, which would have created a dominant chip supplier for cars, smartphones, and basically any product connected to the internet. In a recent statement, Broadcom downplayed the potential threat of antitrust regulators, which have financially and legally battered Qualcomm for months.

Bloomberg reported that Broadcom would resort to a hostile takeover if Qualcomm turned down the deal, which faced lots of skepticism throughout the semiconductor industry. That would mean offering to buy stock from shareholders directly, circumventing management.

The $105 billion bid pitted the ambitions of Broadcom's chief executive Hock Tan—famed as the most voracious dealmaker in the chip industry—against those of Qualcomm's chief executive Steve Mollenkopf, a former chip designer who rose through the ranks of the company he wagers can move its chips into sensors, personal computers, and data centers.

"No company is better positioned in mobile, IoT, automotive, edge computing and networking within the semiconductor industry," Mollenkopf said in a statement. "We are confident in our ability to create significant additional value for our stockholders as we continue our growth in these attractive segments and lead the transition to 5G." ■

JAMES MORRA, Associate Editor



2. Here, a docking mechanism is shown attached to the roof of a vehicle. *(Courtesy of freepatentsonline.com)*

by malicious users. Authentication processes also could be used to confirm whether energy was transferred or not. In addition, it will be possible to confirm the amount of energy that was transferred between the UAV and the vehicle. The UAV location data may be stored in a server to help determine which UAV should be instructed to transfer energy to the vehicle.

An additional feature for the UAV could be an energy storage device, which would be configured to store and release energy for transfer to the vehicle. The energy storage device could store energy in one or more forms including, but not limited to: electrical, magnetic, chemical, or mechanical.

The patent mentions that the UAV could include an energy delivery system comprising one or more mechanisms that control the transfer of energy between the UAV and the vehicle. If the energy storage system includes a battery, the energy delivery system could include multiple mechanical arms configured to hold and release a battery. Either the user could insert the battery into the vehicle or the energy delivery system could be configured to provide energy to the vehicle using any of the various wireless energy transmission techniques (e.g., electromagnetic induction or radiation).

3. An Amazon air delivery drone gets ready for takeoff. *(Courtesy of Amazon)*

AMAZON IN THE AUTOMOTIVE MARKET

The patent itself does not mean that Amazon has a concrete plan to immediately start a new drone car-charging business. At the moment, the electric/autonomous vehicles market is growing at a fast pace. Better infrastructure will be needed to charge these future vehicles. Amazon had already started a new delivery service using drones to deliver packages to customers in 30 minutes or less; why not use them to delivery energy to vehicles, too? ■

MARIA GUERRA, Technology Editor

WILLIAM WONG | Technology Editor

IoT Frameworks: THE TIES THAT BIND

Frameworks and services provide a fast way to deliver IoT products, but there's a catch: It's very hard to build that "walled garden" alone.

Building up frameworks and services to accelerate product delivery for the Internet of Things (IoT) takes lots of time and effort. It also often involves a skill set that developers don't have or want to develop given how difficult it is to concentrate on specific aspects of a solution, be it an IoT end device like a sensor system, a gateway, or an app for a smartphone or embedded controller.

Part of the challenge of moving from a standalone device or one with a limited networking repertoire to an IoT solution is due to the increasing number of hardware and software components needed in a solution—complexity that causes issues in everything from design and debugging to long-term management and security. Issues can range from connectivity to security to latency.

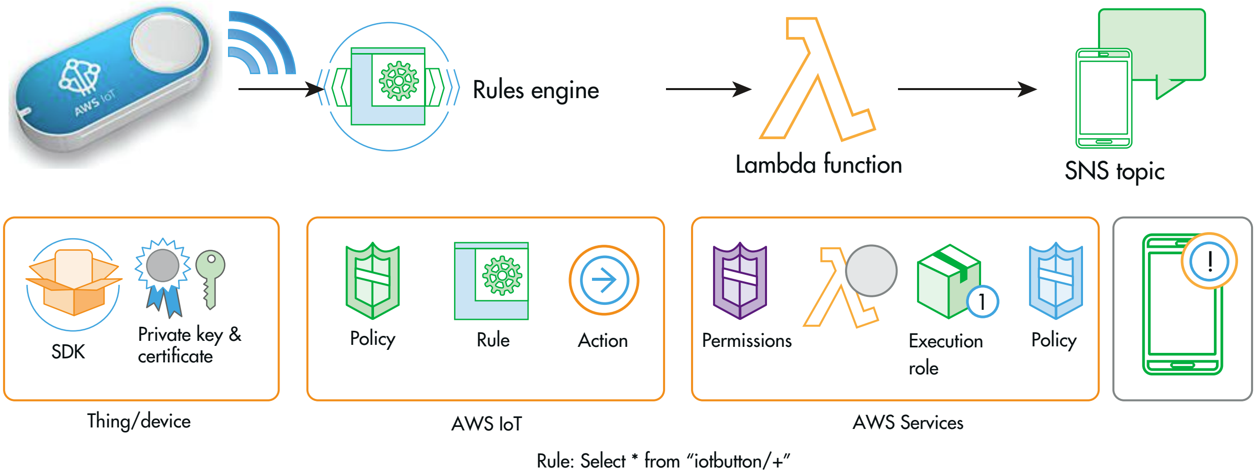
For example, pressing a virtual button on a smartphone running an IoT control app may affect an IoT device. How long this takes depends on a variety of factors, including sending a message up to the cloud and back down to the device. This may be suitable for flipping a light on or off, but might not be fast enough when controlling a drone. On the other hand, a "smart" drone may be able to work well with higher latency, since it would be handling chores like obstacle avoidance and flight stability.

CHOOSING AN IoT WALLED GARDEN

Many companies promise an "end-to-end" IoT solution. They provide stacks running on microcontrollers that link to cloud services. Developers need to incorporate the stack and link their application to it. Services provided by the stack can range from basic communication with the cloud to handling secure over-the-air (OTA) updates.

Regardless of the breadth and depth of support, the IoT solution requires a cloud component, of which there are many options. Some of the big players include Amazon Web Services (AWS) IoT, Microsoft Azure IoT Hub, Google Cloud, Oracle IoT Cloud, IBM Watson Cloud, CISCO IoT Cloud Connect, Salesforce IoT, Bosch IoT Suite, General Electric Predix, and SAP IoT Platform. Some of these provide specialized services such as General Electric's Predix targeted at industrial IoT (IIoT) applications. Many of these organizations provide generic cloud-computing services as well, which often obfuscates the discussion because the IoT services are typically built on top of the computing services.

In general, IoT cloud services tend to be a walled garden. There may be some ability to link IoT entities, including applications, services, or devices, to third-party entities on the same platform. Using data and commands outside of the service is sometimes possible. This may be done using



1. The AWS IoT Button from Amazon is a dongle with a Wi-Fi connection. It's designed to hook into AWS IoT support that can fire off a lambda function running on AWS Services.

remote procedure call (RPC) or representational state transfer (REST)-style interfaces. The protocols involved are as varied as the number of platforms and services.

Just about everyone is getting into the IoT cloud solution mix. For example, Mbed OS and Mbed Cloud are two components of Arm's IoT solution. Arm actually sells intellectual property (IP) for processors and graphics processors. The MbedOS is a lightweight operating system designed to run on low-end Arm microcontrollers. It can actually be used by itself, but it's really designed to support the Mbed protocol stacks to communicate with the Mbed Cloud. The Mbed Cloud provides remote management of devices, including updates. It supports a range of connectivity solutions like the Constrained Application Protocol (CoAP), and can interface with other systems using REST APIs.

Advantech is a major hardware solutions provider. Its WISE-PaaS Alliance partner program includes participants like Microsoft Azure IoT and Arm Mbed. Advantech takes a more modular approach to IoT. Other services in that mix include the WISE-PaaS/SignageCMS, which is a digital signage content-management system. Likewise, McAfee endpoint security and integrity control are additional services developers can utilize on Advantech hardware.

Of course, selling what one already offers is the IoT approach being taken by many. Dell's Edge Gateways for IoT look to bring compute to the edge instead of the cloud. The EdgeX Foundry is an interoperability foundation designed to support Dell's partners, including systems integrators, contractors, and developers.

Having working example always helps, and this even extends to major players like Amazon. Its AWS IoT Button *(Fig. 1)* is a simple Wi-Fi dongle with a button. Though it appears to simply be a button to turn a device on and off, there's much more going on under the covers. As with most secure IoT devices, it has its own private key. The AWS IoT cloud support has rules that are invoked by clicking the button. These, in turn, initiate a lambda function in a "serverless" cloud environment. The serverless environment essentially runs small applications within a secure environment that is lightweight even for containers. Rules and lambda functions are yet another new idea for many developers to contend with.

IoT frameworks or collaboration can align along components of the system like LoRa Alliance's LoRaWAN. One way to connect LoRaWAN devices to the cloud is to use the The Things Network (TTN). Another is to use Comcast's machineQ service. These highlight how the choice of an underlying wireless technology can dictate the IoT framework options available to developers. These services normally terminate in a cloud service like Amazon AWS IoT or Microsoft Azure IoT.

Almost all frameworks will note that they're "built on standards," but that normally means they use standard communication stacks like TCP/IP and may build on these with protocols like MQTT. Quite a bit more is involved with IoT communication, since everything from security to service and device discovery is part of the overall communication protocol. Much of this higher-level communication tends to be non-standard. Usually, that means two different IoT frameworks can coexist on the same network and communication infrastructure, but are islands unto themselves.

THE VOICE CONNECTION

Voice control just adds another wrinkle into the IoT framework walled garden mix. The "smart speaker" craze is fueled by platforms like Apple's HomePod, Amazon's Echo/Alexa, Microsoft/Harman Kardon's Cortana, and Google's Google Home *(Fig. 2)*. These consumer devices recognize a user's voice commands, which are analyzed in the cloud.

2. Apple's HomePod (a), Amazon's Echo (b), Microsoft/Harman Kardon's Cortana (c), and the Google Home (d) smart speakers are building the audio walled gardens.

Voice control just adds another wrinkle into the IoT framework walled garden mix. The "smart speaker" craze is fueled by platforms like Apple's HomePod, Amazon's Echo/Alexa, Microsoft/Harman Kardon's Cortana, and Google's Google Home.

Auditory feedback, such as answering a question or playing music, can be handled by the speakers. However, commands can invoke other actions associated with other IoT devices like smart lightbulbs or washing machines. Even security systems and other types of systems can be controlled by a voice-based solution.

Such frameworks provide a level of configuration and interoperability that normally crosses the other IoT frameworks for non-smart speaker devices. The interaction is typically in the cloud with the onus placed on the developer to make the connection between their service and the smart speaker service. Amazon calls these Alexa "skills."

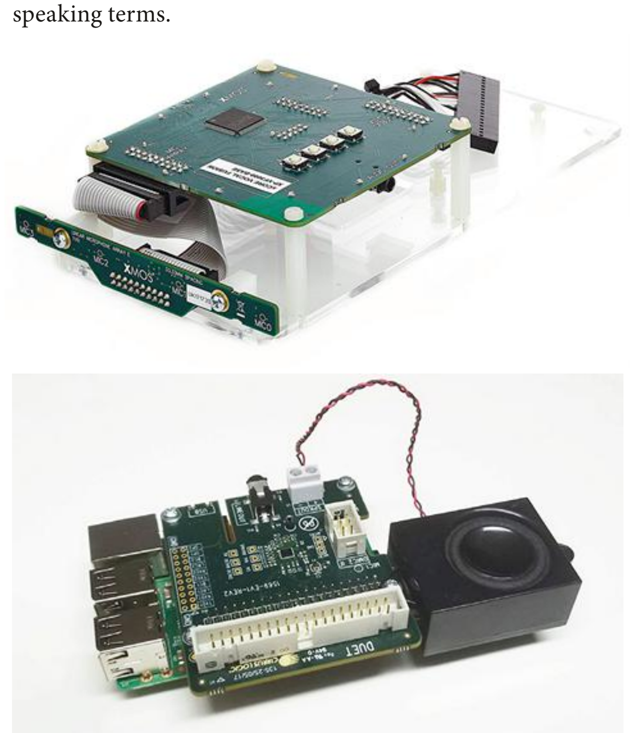
Requiring a smart speaker for your IoT device is probably not a great idea, but it's possible to incorporate that technology into things like a voice-managed washing machine. I have tried a number of development kits that work with Amazon's Alexa Voice Service (AVS). This includes XMOS's xCORE VocalFusion 4-Mic Kit and Cirrus Logic's Alexa Voice Capture Development Kit for Amazon AVS *(Fig. 3)*. Both hook up to AVS and provide the same functionality as an Amazon Echo. They can process voice commands and play back responses and music. Each requires a free Amazon Developer account.

XMOS's platform uses the multicore xCORE VocalFusion processor to handle the audio-processing chores. Developers will also need to obtain and install a Rasberry Pi 3 plus power supply along with a speaker. The system has a four-PDM (pulse density modulation) microphone array that handles far-field processing.

Cirrus Logic equips the Raspberry Pi 3 with a kit to link its CS47L24 smart codec to the internet. The system is designed for low-cost applications using a pair of CS7250B digital MEMS microphones. The company also has a graphical, web-based interface that makes setup and configuration significantly easier. On top of that, it offers solutions that handle more microphones for higher-end platforms.

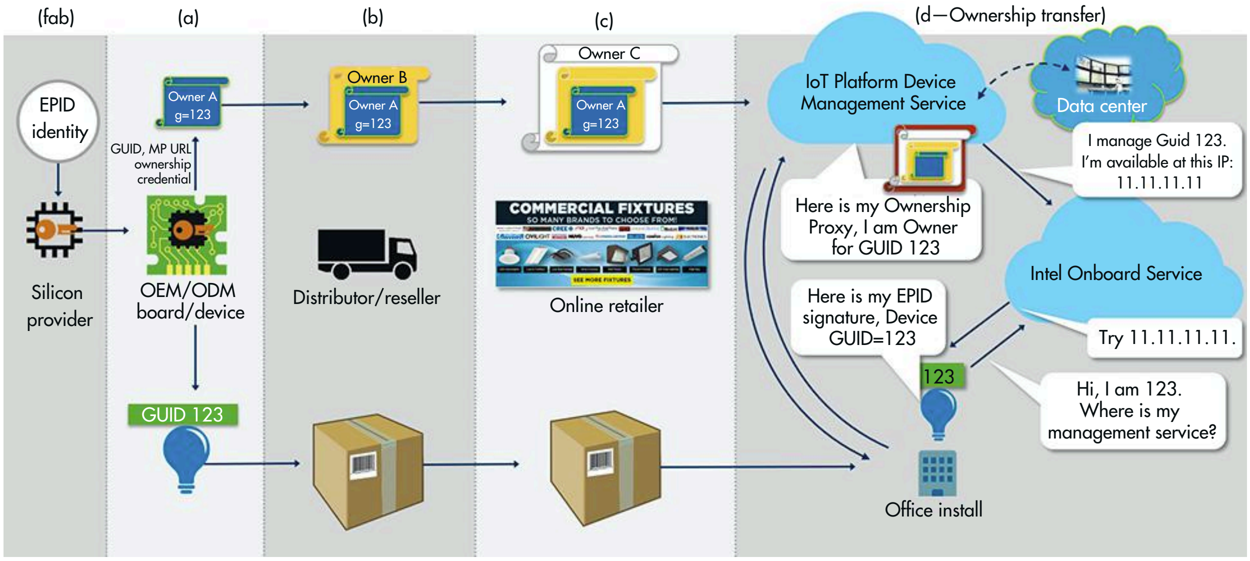
In general, the Raspberry Pi is overkill for handling the AVS support. It does offer a good platform for implementing other services, although the device would typically implement a "skill" that could be initiated via AVS while sharing the network connection and providing communication support for the codecs. Developers looking to implement local voice control will face a tougher challenge.

This type of voice command support is going to wind up in everything from television sets to refrigerators. The challenge for developers is which one to support, since consumers will likely want to have all of their devices work together and the creators of the vocal walled gardens aren't really on speaking terms.



3. XMOS's xCORE VocalFusion 4-Mic Kit (a) and Cirrus Logic's Alexa Voice Capture Development Kit for Amazon AVS (b) provide Alexa-enabled smart speaker support.


HELPING YOU
DO THE
ELECTRIC SLIDE
MPD DEVICES CAN BE FOUND IN CARS
AROUND THE WORLD
BATTERYHOLDERS.COM



4. Secure Device Onboard (SDO) developed by Intel securely links a device to a cloud service when it's initially set up.

Voice control is only one type of service for an IoT solution that will likely be handled in the cloud. Artificial intelligence (AI) and machine learning (ML) tends to require more horsepower and data, making it a useful adjunct to a local IoT device. The smart speakers are already using this for voice recognition and natural language processing. For example, Watson is part of IBM's solution.

DISCOVERING IoT

The initial connection between an IoT device and a cloud-based service using the various developer's kits is designed to be flexible but not necessarily simple, whereas a final consumer or industrial device needs to have a very easy installation process. Some IoT frameworks provide this type of service.

Another possibility is Intel's Secure Device Onboard (SDO) approach *(Fig. 4)*. SDO assumes that the chip supplier has secure hardware support built-in, including an Enhanced Privacy ID (EPID)—essentially a private key. The device and its EPID are paired with a 128-bit Globally Unique Identifier (GUID) that's usually presented on a bar code associated with the device. The GUID is used to tell the SDO server what service will handle the device. The EPID and other keys make sure the transaction is secure and authenticated.

The SDO support is only used when a device is initially provisioned or if it needs to be reprovisioned. The latter can occur if the device is sold or set to other uses.

IoT devices may be designed to simplify set up and use by consumers and companies, but it's complex: Everything from provisioning to long-term management is in the mix. Even something as simple as the AWS IoT Button involves a lot of software for any transaction, even though it's simply linked to another IoT device to turn it on and off. Doing all of this securely and reliably is what makes the development process interesting.

MARIA GUERRA | Analog/Power Editor

DLP and Laser Options Give Drivers a Heads-Up

Head-up displays are becoming a centerpiece in automotive design, as different display technologies evolve to give the driver an immersive infotainment experience.

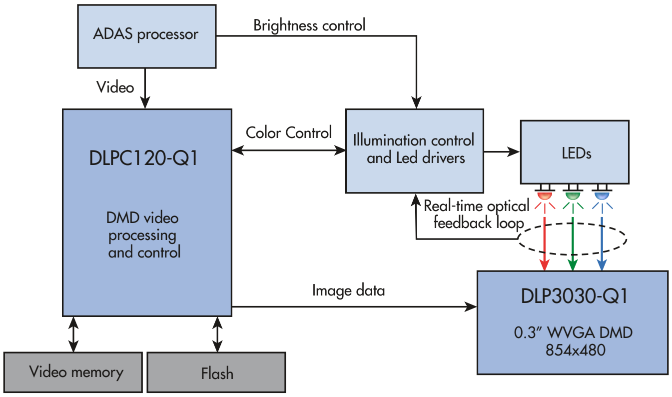
Head-up displays (HUDs) were initially developed for defense aviation many decades ago. Today, the technology is quickly evolving in automotive applications to give drivers information such as navigational data on a transparent screen right in the driver's line of sight *(Fig. 1)*. A key element of data displayed by HUDs is that they are presented in a way that does not distract drivers. A market report from BCC Research states that the market for HUD components is expected to grow to $8 billion by 2022 from $2.7 billion this year. The following two options, which are being used by automotive original-equipment-manufacturer (OEM) developers, rely on cutting-edge technologies to improve the driver's experience.

DIGITAL LIGHT PROCESSING (DLP)

DLP is a display device technology based on optical micro-electromechanical systems (MEMS). At its heart is a digital micromirror device. For example, Texas Instruments has taken the technology behind its DLP Cinema projection product and qualified it for automotive applications. The chipset consists of highly reflective, digitally switchable, micrometer-sized mirrors (micromirrors). The micromirror array consists of 608 micromirror columns by 684 micromirror rows in a diamond pixel configuration. Each individual micromirror is positioned over a corresponding CMOS memory cell. The angular position of a specific micromirror is determined by the binary state (logic 0 or 1) of the corresponding CMOS memory cell contents after the mirror clocking pulse is applied.

The company's chipset (DLP3000-Q1) targets a wide field of view and augmented-reality HUD applications with a field of view reaching 12 × 5 deg. The chipset family consists of a DLP 0.3-in. wide video graphics array (WVGA) digital micromirror device (DMD) and DLPC120 controller *(Fig. 2)*. The controller is responsible for accepting the video input and formatting the data to display on the DMD while simultaneously controlling RGB light-emitting diodes (LEDs) in order to create a real-time image. The DLP also controls the power-up and power-down events of the DMD according to external system control or temperature input from the DMD.

1. Shown is a head-up display feature in the 2017 Lincoln Continental. *(Courtesy of Texas Instruments)*



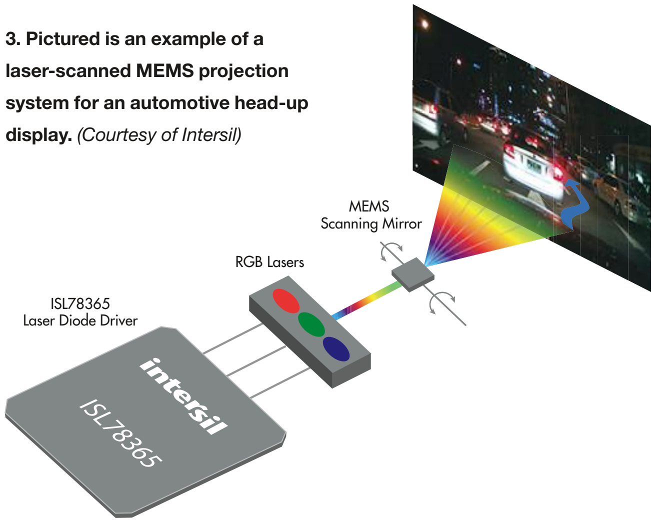
2. With this chipset, automakers and Tier 1 suppliers can reportedly design HUDs with Virtual Image distances to 20 meters. *(Courtesy of Texas Instruments)*

LASER-SCANNED MEMS PROJECTION DISPLAY

In a laser-scanned MEMS projector, each pixel is pulsed very rapidly to create the full high-definition resolution. Because the laser beam is always in focus, the image can be projected into the windshield without requiring refocusing optics. This greatly reduces the overall optical system complexity and size, eliminating costly optical components and assembly.

A laser-scanned MEMS HUD consumes electrical power when there are relevant pixels to be projected. With the typical navigation and instrumentation information, most of the electrical energy is consumed when there is a need to put a pixel onto the display. This dramatically reduces the electrical requirement, resulting in a lower thermal profile and thus smaller thermal dissipation requirements.

Intersil's ISL78365 is an AEC-Q100 Grade-1 qualified laser diode driver that pulses four high-intensity lasers up to 750 mA for projecting full HD color video onto the windshield *(Fig. 3)*. The chip supports a wide variety of color laser-diode configurations, allowing system designers to achieve the desired brightness, contrast, and rich color image. To meet the thermal requirements, the device offers three power-saving modes for high efficiency and low power losses.



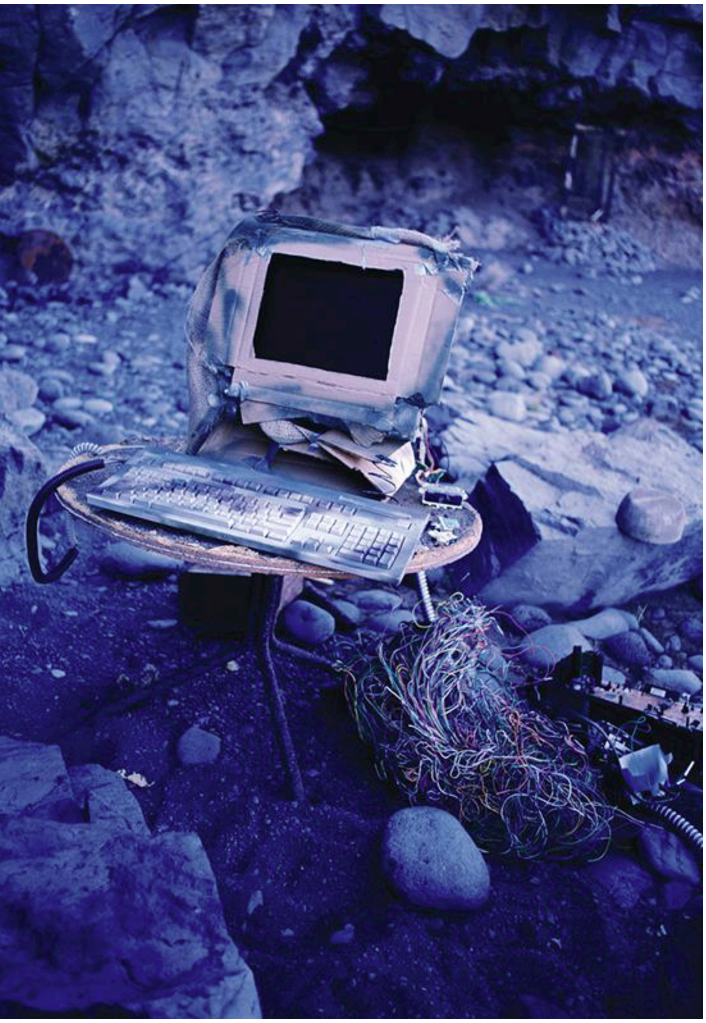
3. Pictured is an example of a laser-scanned MEMS projection system for an automotive head-up display. *(Courtesy of Intersil)*

These two technologies are among the many options that automotive OEM developers are considering. Several factors are considered when deciding which one to use, like the amount of content on the display, brightness, dimming range, supplied power, size,and—last, but not least—the cost of the solution. As prices for HUDs fall, we will start to see a migration of this technology from luxury cars to more affordable car options. ed

ANTHONY BUDRANT | Senior Engineering Manager, Dell

11 MYTHS ABOUT Ruggedization and Testing to Enable IoT

Internet of Things products must be able to take the heat, so to speak, and go through multiple test cycles, but the techniques used have developed some mythical traits.



A solid IoT solution encompasses a lot of working parts, and at the front end of that is developing the hardware. Marketing needs to have a firm understanding of functional and environmental requirements, and engineering must be inventive and thorough enough to incorporate all of these into the product. But the real fun begins once the first prototypes have been created and the product-development test labs start taking them through their paces.

Successful products in this space aren't invented through an "armchair quarterback" approach, but rather ground into existence through the "elbow grease" iterations of create, test, break, fix, and repeat. Some interesting myths have developed over the years around these ruggedization and testing processes, and it's high time that they be debunked.

1. ALL THERMAL CHAMBERS ARE CREATED EQUAL.

Visit almost any electronic hardware testing laboratory and chances are you will encounter several large thermal chambers noisily humming along. They work much like your air conditioning at home—a large compressor and furnace in the bottom and several fans that swirl the heated or cooled air around in the chamber area on top, where units to be tested are placed.

The purpose of the fans is to swirl the air around inside the chamber to ensure a uniform temperature gradient. These work great for testing hardware that's actively cooled (i.e., have fans or blowers that move air through a heat exchanger), but they don't work well for passively cooled items (no fan, just large-finned heat sinks that rely on natural convection to move heat away from the hardware).

Why don't they work well for passively cooled hardware? The answer lies in all of that swirling air from those fans. For actively cooled hardware, the effect of the swirling air on thermal transfer is negligible compared to the internal fan/blower ramming air through a heat exchanger. For passively cooled hardware, the effect is too large to ignore. And worse, the data that you get is not conservative, meaning you could have the hardware pass the test in your thermal chamber but fail in the real world. Not a good situation!

Fortunately, there is a good solution: natural convection chambers. These chambers heat the testing chamber via infrared heaters and are designed to vent so that there's no moving air. When the unit under test passes 70°C (as an example) in one of these chambers, you can feel confident that it will perform as intended, even in an installation closet of dead still air.

2. TESTING TO THE SPECIFICATION LIMIT IS GOOD ENOUGH.

In most test labs, there's a lot of focus on passing the specification. Emphasis is placed on having a "statistically significant" sample size and calculating confidence levels. All of this is absolute goodness, but in my opinion doesn't replace the need to explore how much margin is in your product. All of the reliability in the world at the stated spec limit won't save your bacon the day your enclosure fan goes out, or one of the pieces of equipment decides to overheat and drive up the ambient temperature for everything else in the cabinet, or… well, you get the idea.

Another important reason to explore margin is that it gives insight into your weakest link. And oftentimes, it might be quite cost-effective to make a change that dramatically improves the margin of your product. If this sounds like an echo of the Highly Accelerated Life Testing advocated by Dr. Gregg Hobbs back in the late 1980s and 1990s, you're exactly right. It's not a new idea, but still a powerful one.

3. DUST TESTING ISN'T IMPORTANT UNLESS YOU'RE DEPLOYED IN THE DESERT.

Dust isn't restricted to the desert. It turns out it is all around us most of the time, and it can definitely affect the performance of your electronics by lowering its ability to get rid of heat.

But what about dust that contains a high level of pollution? Now you need to worry about how well your electronics can resist corrosion. What if you're deploying the product in a machine shop or anywhere else where there's a lot of conductive particulate in the air? Now you should be concerned about electrical shorting on the printed wiring boards of your electronics. Dust comes in several flavors, and you need to be aware of how your product is going to operate when it's deployed in those environments.

4. ONE SIZE VIBRATION PROFILE FITS ALL.

When we talk about where IoT devices can be deployed, I always think about that old Steve Martin movie *Planes, Trains, & Automobiles*. It probably won't take much effort to convince most people that the vibration profile on a train is quite different from that on a plane or in an automobile. Shipping on the water brings in yet another mode. But it is much more complicated than just sorting into four or five groups.

Take automotive as an example. You're going to get a very different profile under the passenger seat of the cab of an 18-wheeler as compared to being mounted on the wall of the trailer it's pulling. What if you're deployed under hood somewhere in the engine compartment? There are lots of profiles to examine for your IoT product, and you need to be testing the relevant ones for your customers.

5. IT DOESN'T MATTER IF YOU EXERCISE THE HARDWARE DURING YOUR ENVIRONMENTAL TESTING.

What if I wanted to sell you a car and told you that the engine didn't overheat as long as you left it in park? Still interested? IoT hardware is deployed to perform some function or even multiple functions. It only makes common sense that you would put the hardware through its functional paces while doing the environmental testing to see how it handles the workload.

As an example, a gateway may run great at 70°C as long as it isn't processing any sensor signals, but throttle significantly when it has to process a large number of them. An important part of IoT testing is to characterize the hardware responses to these kinds of stimuli and test for worst-case workloads.

6. ALL BENCHMARKS GIVE THE SAME BASIC DATA.

Benchmarks are wonderful in that they allow us to compare different things, but you must be careful with those comparisons. For instance, you wouldn't take a Windows-based benchmark and then assume that it holds for a Linux system. Yet the pressure is there to do just that since there aren't a lot of Linux-based benchmark tools available.

You also need to know what parameters are being exercised by the benchmark. It won't do you much good to buy an IoT product that has a great benchmark score if it turns out the benchmark doesn't exercise heavy I/O traffic and you want to use it to process a large array of sensors.

7. DISCOVERING PRODUCT PERFORMANCE MARGIN ISN'T IMPORTANT.

Starting to get an idea that I'm a big fan of understanding product margin? Again, it's important to understand the limits of the product under investigation so that you can have intelligent conversations around solving someone's challenges.

What happens when someone has a special installation (aren't they all) and the discussion turns to the obvious question: Will the hardware handle it? Or what if they want to double the number of sensors they want to monitor, but are only going to 60°C instead of 70°C? Of course, you may not have time to explore every combination of temperature, I/O load, computational load, etc. However, you want to try and book-end several of these in order to have intelligent conversations about how your hardware is going to respond to the myriad of potential customer scenarios.

8. COMPONENTS AREN'T AS IMPORTANT AS OVERALL DESIGN.

What is that old wise saying: You are only as strong as your weakest link? This especially holds true for electronics. All of those capacitors, resistors, and inductors are put into the design for a reason, and you can bet that when one or more of them dies off, you will experience performance degradation.

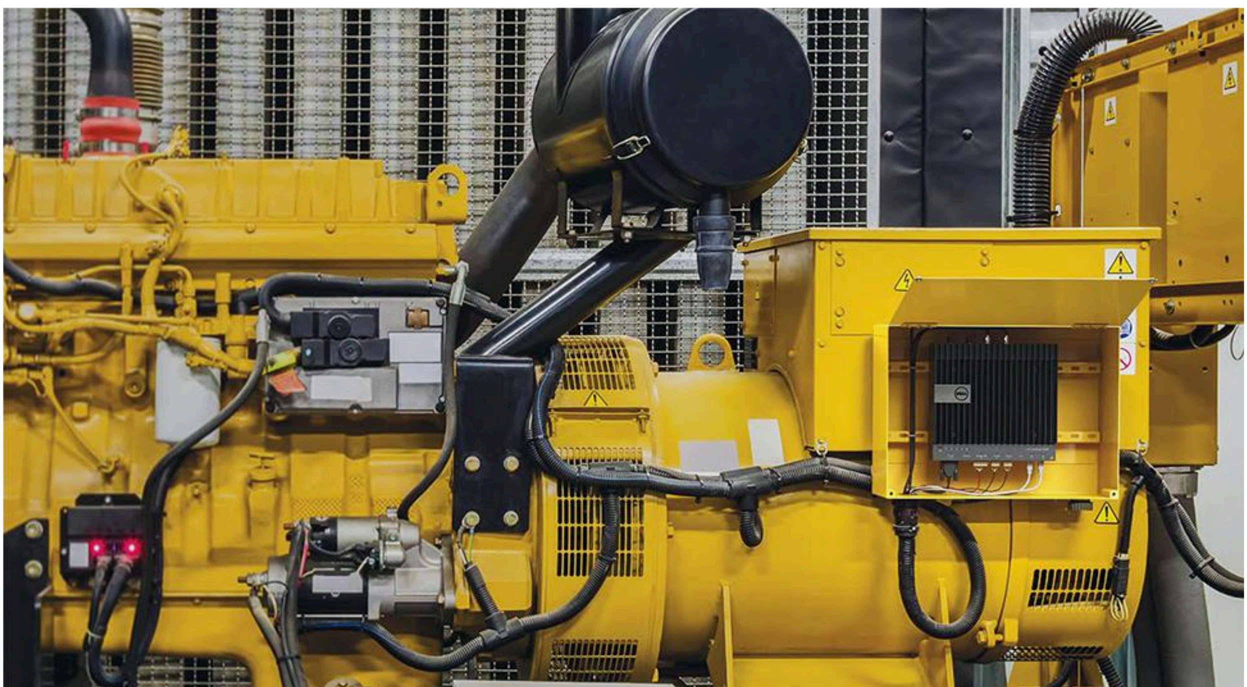
The worst case is that they fail under thermal load, but perform adequately at room temperature when the tech is trying to troubleshoot them. This can end up wasting a lot of time as the hardware cycles back and forth between failing in the field and being labeled CND (Could Not Duplicate) in the failure analysis lab, only to be sent out to the field again to start the cycle anew. The message is that you want the hardware to have been designed and stuffed with high-end components, not the cheapest thing that could be found to try to save a few cents here or there.

9. EVERYTHING CAN BE FIXED WITH A SOFTWARE UPDATE.

When ruggedizing IoT hardware, you spend a significant amount of time worrying about thermal and vibration performance. You also are taking a hard look at functionality and how it stands up in different environments. It's an iterative process and many improvements get put into the product during this testing. Examples include upgraded TIM (thermal interface material), more heat pipes, additional seals, certain components being glued down to the printed wiring board to make it more robust in the vibration environment, etc. Reviewing that list, how many of them do you think you'll be able to fix with a software upgrade? You need to design, manufacture, and test it before it ever sees a customer's hands, so that you don't end up trying to sell the "software update" story.

10. LAB TESTING IS THE END OF PRODUCT EVALUATION.

Testing in the lab is a very important element of developing a high-quality product, but it isn't the final chapter. A lot of thought, research, and data collection goes into this testing,



Here, an IoT gateway is mounted in a thermally and vibrationally challenging environment.

PICO

The big name in miniature components.

Transformers & Inductors, DC-DC Converters, AC-DC Power Supplies

The most demanding applications require the world's most reliable components. For over 50 years PICO Electronics has been providing innovative COTS and custom solutions for Military, Commercial, Aerospace and Industrial applications. Our innovative miniature and sub-miniature components are unsurpassed in any industry. PICO Electronics' products are proudly manufactured in the USA and are AS9100C Certified.

To learn more about our products and how you can benefit from our expertise visit our website at picoelectronics.com or call us today at 800-431-1064.

think... low profile from .18" ht.

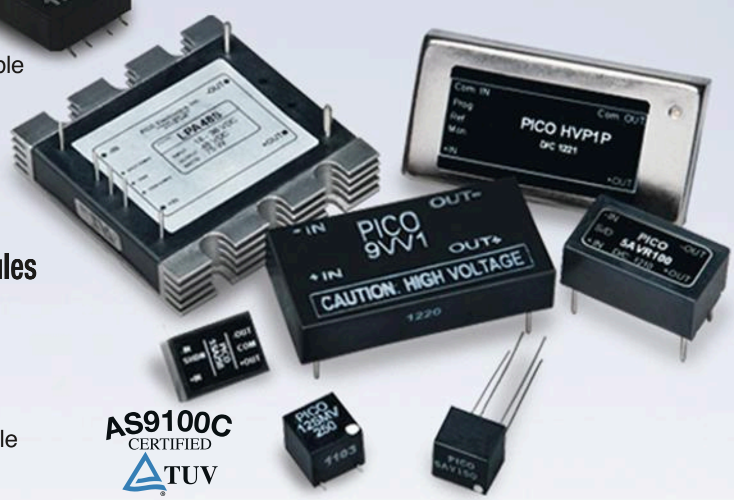
TRANSFORMERS & INDUCTORS

Think Pico Small - Over 5000 std Ultra Miniature

- Ultra Miniature Designs
- MIL-PRF 27/MIL-PRF 21038
- DSCC Approved Manufacturing
- Audio/Pulse/Power/EMI Multiplex Models Available
- For Critical Applications, Pico Continues to Be the Industry Standard

Surface Mount & Thru Hole

Military • COTS • Industrial



DC-DC CONVERTERS

2V to 10,000 VDC Outputs — 1-300 Watt Modules

- MIL/COTS/Industrial Models
- Regulated/Isolated/Adjustable Programmable Standard Models
- New High Input Voltages to 900VDC
- AS9100C Facility/US Manufactured
- Military Upgrades and Custom Modules Available

AS9100C CERTIFIED TUV

VISA MasterCard AMERICAN EXPRESS

PICO Electronics Inc.
143 Sparks Ave, Pelham, NY 10803
Call Toll Free: 800-431-1064
E Mail: Info@picoelectronics.com • FAX: 914-738-8225

VISIT OUR EXCITING NEW WEBSITE: www.picoelectronics.com

but it's still a proxy for what you really want to know—how will it perform in the real world.

To that end, it's important to embrace some form of early evaluation program into your product development. You want people who are actually trying to solve their problem exercising your hardware, using it in the manner that works and makes sense for them. Because, inevitably, they will find something that you didn't discover in the lab, and it's much better and cheaper to find out about it before you mass deploy.

11. I DON'T HAVE TO WORRY ABOUT QUALITY AS LONG AS I HAVE A GOOD WARRANTY.

This myth is a very old one, and pre-dates modern electronics. The theory is that if I can buy two of product X for the cost of one product Y, I come out ahead the minute my second product X lasts longer than the aforementioned Y, and it's all gravy after that point. The fallacy is that you aren't factoring in the cost of recovering from the failure of product X, as well as the cost of deploying the second product X. These costs aren't trivial, especially in some IoT solutions.

If your sensor or gateway is located on a pipeline smack in the middle of nowhere, 100 or more miles from the nearest small town and twice that far from the closest service technician, the cost of failure can way outstrip the purchase price of

You want people who are actually trying to solve their problem exercising your hardware, using it in the manner that works and makes sense for them.

the product itself. (The service council estimates an average truck roll is $286 plus $79/hr for labor.) Not to mention the thousands of gallons of oil you might be on the hook to clean up because your sensor didn't catch the break.

This is an extreme example, but the point is a solid one. You need a good understanding of the situation and environment that your solution is being deployed in order to understand where you're going to want to fall on the cost-quality continuum. ed

ANTHONY BUNDRANT, Senior Engineering Manager at Dell, is currently responsible for the Rugged Mobility, Internet of Things, and Design to Value labs in Austin, Texas. He has been an engineer working in electronic hardware product development for over 20 years. When not breaking things in the lab, he enjoys riding road and mountain bikes, reading, and operas.

NICK NI | Senior Product Manager at Xilinx
ADAM TAYLOR | President of Adiuvo Engineering and Training

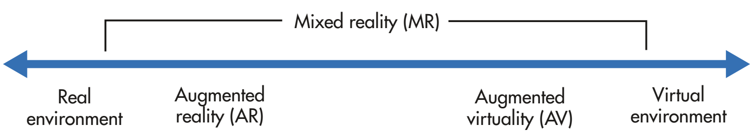
Streamline Your Augmented-Reality System with an All-Programmable SoC

As AR gains more prominence throughout industrial and consumer environments, solutions for these complex systems need to be more integrated yet still handle the huge data-processing loads.

Research has shown that we humans interact with the world visually since we process visual images many times faster than information presented in other forms, such as written text. Augmented reality (AR), like its virtual-reality (VR) cousin, enables us to experience an increased perception of our surrounding environment. The major difference is that AR adds to, or augments, the natural world with virtual objects such as text or other visuals, equipping us to interact safely and more efficiently within our natural environment, whereas VR immerses us within a synthetically created environment.

Combinations of AR and VR are often described as presenting us with a mixed reality (MR) *(Fig. 1)*. Many of us may have already used AR in our everyday lives without necessarily being aware, such as when we use our mobile devices for street-level navigation or to play AR games like Pokémon Go.

One of the best examples of AR and its applications is the head-up display (HUD). Among simpler AR applications, HUDs are used in aviation and automotive applications to make pertinent vehicle information available without glancing at the instrument cluster. AR applications with more advanced capabilities, including wearable technologies (often called smart AR), are predicted to be worth $2.3 billion by 2020, according to Tractica.



1. Combining augmented reality and virtual reality creates a mixed reality.

AUGMENTED REALITY ENHANCES OUR LIVES

AR is finding many applications and use cases across industrial, military, manufacturing, medical, and commercial sectors that enhance our lives. Within the social commercial sphere, AR is used in social-media applications to add biographical information and even recognize each person.

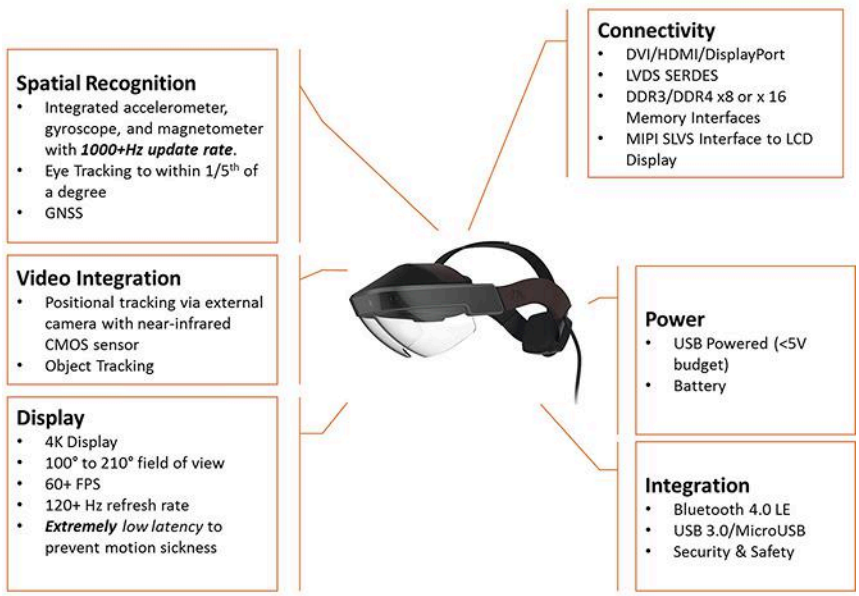
2. Here's an example of smart glasses used in an industrial setting.

Many AR applications are based around the use of smart glasses worn by an operative. These smart glasses help to increase efficiency within the manufacturing environment by replacing manuals or by illustrating how to assemble piece parts *(Fig. 2)*. In the medical field, smart glasses have the potential to share medical records as well as wound and injury details, thus giving on-scene emergency services the benefit of information that can later be made available to the ER.

Most AR systems are also portable, untethered, and, in many instances, wearable, as is the case with smart glasses. This creates the unique challenge of implementing the processing required within a power-constrained environment.

A large parcel-delivery company is currently using AR in smart glasses to read the bar code on shipping labels. Having scanned the bar code, the glasses can communicate with the company's servers using Wi-Fi infrastructure to determine the resultant destination for the package. With the destination known, the glasses can indicate where the parcel should be stacked for its ongoing shipment.

In addition to considering the end application, AR solutions involve a number of requirements, including performance, security, power, and future-proofing. Some of these can be competing, so designers must consider all of these requirements to arrive at the optimal AR system solution.



3. Looking at the anatomy of an augmented-reality system, multiple sensors are used, such as MEMS accelerometers and gyroscopes.

EMPOWERING AR SYSTEMS TO SUCCEED

Complex AR systems require the ability to interface to, and process data from, multiple camera sensors that understand the surrounding environments. These sensors may also operate across different elements of the electromagnetic (EM) spectrum, such as infrared or near infrared. In addition, sensors may furnish information from outside the EM spectrum, providing inputs for detection of movement and rotation, as with MEMS accelerometers and gyroscopes, along with location data dispensed by Global Navigation Satellite Systems (GNSS) *(Fig. 3)*. Embedded-vision systems that perform sensor fusion from several different sensor types like these are commonly known as heterogeneous sensor-fusion systems.

AR systems also require high frame rates along with the ability to perform real-time analysis frame-by-frame to extract and process the information contained within each frame. Equipping systems with the processing capability to achieve these requirements becomes a driving decision factor in component selection.

An example of a single chip that has the capability to process cores for AR systems is Xilinx's All Programmable Zynq-7000 SoC or Zynq UltraScale+ MPSoC. These SoCs are themselves heterogeneous processing systems that combine ARM processors with high-performance programmable logic. Zynq UltraScale+ MPSoC, the next generation of the Zynq-7000 SoC, also incorporates an ARM Mali-400 GPU. In addition, certain family members contain a hardened video encoder that supports H.265 and the high-efficiency video coding (HEVC) standard.

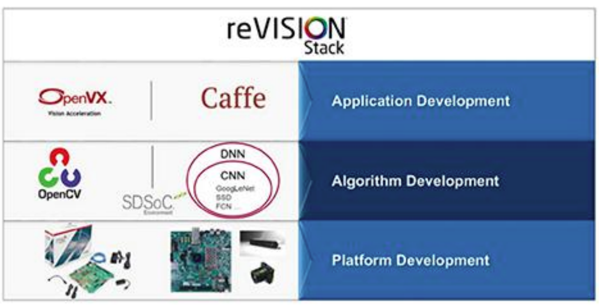
These complex devices enable designers to segment their system architectures using processors for real-time analytics and transferring traditional processor tasks to the ecosystem. Designers can utilize the programmable logic for sensor interfaces and processing functions. This brings benefits such as:

- Parallel implementation of N image-processing pipelines as required by the application.
- Any-to-any connectivity—the ability to define and interface with any sensor, communication protocol, or display standard—allowing for flexibility and future upgrade paths.

SUPPORT FOR EMBEDDED VISION AND MACHINE LEARNING

To implement an image-processing pipeline and sensor-fusion algorithms, developers can leverage the reVISION acceleration stack that supports both embedded-vision and machine-learning applications. Developed predominantly within the software-defined SoC or SDSoC toolset environment, reVISION permits designers to use standard frameworks such as OpenVX for cross-platform acceleration of vision processing, OpenCV computer vision library, and Caffe Flow to target both the processor system and programmable logic. The reVISION stack can accelerate a large number of OpenCV functions (including the core OpenVX functions) into the programmable logic.

Furthermore, reVISION supports implementation of the machine-learning inference engine within the programmable logic directly from the Caffe prototxt file. The ability to use industry-standard frameworks reduces development time: It minimizes the gap between the high-level system model and design completion while yielding a more responsive, power-efficient (pixel per watt) and flexible solution thanks to the processing system and programmable logic combination *(Fig. 4)*.



4. Using industry-standard frameworks reduces development time.

Designers must also consider the unique aspects of AR systems. They're not only required to interface with cameras and sensors that observe the surrounding environment and execute algorithms as needed by the application and use case, but they must also be capable of tracking users' eyes, determining their gaze and, hence, where they're looking.

This is typically accomplished by using additional cameras that observe the user's face and implementing an eye-tracking algorithm that allows the AR system to follow the user's gaze and determine the content to be delivered to the AR display. This promotes efficient use of the bandwidth and processing requirements. Performing such detection and tracking can be a computationally intensive task, but it's possible to accelerate it using reVISION.

PRIORITIZING POWER FOR PORTABLES

Most AR systems are also portable, untethered, and, in many instances, wearable, as is the case with smart glasses. This creates the unique challenge of implementing the processing required within a power-constrained environment. In this case, both the Zynq-7000 SoC and Zynq UltraScale+ MPSoC families rank in the top echelon in terms of performance per watt, according to Xilinx. They can further reduce power during operation by exercising different options, ranging from placing processors into standby mode to be awoken by one of several sources to powering down the programmable logic half of the device. By detecting that they're no longer being used in these instances, AR systems extend battery life.

During operation of the AR system, elements of the processor not currently being used can be clock-gated to reduce power consumption. Designers are able to achieve a very efficient power solution within the programmable logic element by following simple design rules, such as making efficient use of hard macros, careful planning of control signals, and considering intelligent clock gating for device regions not currently required. This provides a more power-efficient and responsive single-chip solution when compared with a CPU or GPU based approach.

A single-chip Zynq-7000 SoC or Zynq UltraScale+ MPSoC solution using reVISION to accelerate machine-learning and image-processing elements achieves between 6X (machine learning) and 42X (image processing) more frames per second per watt with one-fifth the latency compared to other GPU-based solutions.

MEETING SENSITIVE SECURITY DEMANDS

AR applications such as sharing patient medical records and manufacturing data call for a high level of security both in the information-assurance (IA) and threat-protection (TP) domains, especially as AR systems will be highly mobile and could be misplaced. IA requires that we can trust the information stored within the system along with information received and transmitted by the system.

For a comprehensive IA domain, designers can leverage the Zynq devices' secure-boot capabilities that enable the use of encryption. They also need to perform verification using the advanced encryption standard (AES), keyed-hash message authentication code (HMAC), and RSA public key cryptography algorithm. Once the device is correctly configured and running, developers can employ the ARM TrustZone and hypervisors to implement an orthogonal world, where one is secure and can't be accessed by the other.

When it comes to threat protection, designers could use the built-in Xilinx ADC (XADC) macro within the system to monitor supply voltages, currents, and temperatures, and detect any attempts to tamper with the AR system. Should a threatening event occur, the Zynq device has protective options ranging from logging the attempt to erasing secure data and preventing the AR system from connecting again to the supporting infrastructure.

For more information, check out *http://www.xilinx.com/products/design-tools/embedded-vision-zone.html.*

JACOB BABCOCK | Co-founder and CEO, NuCurrent

What's the Difference Between Qi and Other Types of Wireless Power Transfer?

Interoperability, adoption, use case, readiness, and safety/regulatory are the key differentiating factors among these competing technologies.

Apple announced that its iPhones, AirPods, and other accessories will all include Qi (pronounced "chee") wireless charging. The Qi standard is one type of wireless power transfer, and certain to be a popular one due to Apple's adoption. However, other types of wireless power transfer, such as AirFuel Resonant, proprietary near-field magnetic coupling (NFMC), radio frequency (RF), and ultrasound offer different value propositions.

The purpose of this article is to explain the key differences between Qi and other types of wireless power transfer technologies. The focus is on interoperability, adoption, use case, technology readiness, and safety and regulatory.

NuCurrent's high-efficiency wireless power solutions are frequency-independent and frequency-compliant across the Wireless Power Consortium (Qi) and AirFuel Alliance.

INTEROPERABILITY

The No. 1 value-added differentiator for Qi is interoperability. If you see the Qi logo on a product, it is Qi-certified. Qi-certified devices (e.g., phones) are guaranteed to work with Qi-certified transmitters (e.g., charge pads, enabled autos, embedded furniture). This is important in the world of consumer electronics, where users can expect to have Qi transmitters in common locations throughout their daily life: home, car, office, coffee shops, airports, hotels. For the foreseeable future, the vast majority of consumer electronics will be Qi devices due to the benefits of interoperability and leveraging a common infrastructure.

AirFuel is another standard that offers interoperability using a different type of protocol, frequency, and process than Qi. Theoretically, AirFuel promises the same interoperability benefits as Qi (all AirFuel devices will work with all AirFuel transmitters), but the current reality is that Qi has scale via adoption that AirFuel can't match.

Proprietary NFMC is, by definition, "proprietary" or "non-interoperable" with other devices. Proprietary systems don't make sense for consumer mobile devices, but make a lot of sense for non-consumer devices like medical tools/devices, commercial-grade equipment, industrial electronics, unique form-factor devices, etc. There are at least three specific reasons why products may not want interoperability:

1. Device security
- Eliminate workers from charging their work devices in a public space and forgetting them
- Exposing devices to data vulnerability through public infrastructure

2. Safety
- Safety hazards caused by using personal devices on work equipment (e.g., delivery drivers charging personal cellphones on auto transmitters meant for handheld inventory trackers)

3. Unique use cases
- The Qi and AirFuel standards have specific use-case constraints that don't suit all applications

RF and ultrasound are each in very early stages of development. Individual companies are launching "standards" (such as Ossia's "Cota Standard"), but the standards are unlikely to become ubiquitous without much broader sup-

The main value of Qi is that it's interoperable and going to be everywhere. The main limitation of Qi is the use case. Qi relies on tightly coupled technology, low frequency, and limited in-band communication.

port from ecosystem partners and further technology readiness. Interoperability is theoretically possible, but years away due to the time and cooperation involved in real standards development.

ADOPTION

Qi technology is undoubtedly the leader in number of mobile devices deployed worldwide. Apple, Google, HTC, LG, Motorola, Nokia, and Samsung have launched Qi mobile phones (note: Google added Qi for Nexus 4, but dropped it from future models citing "slow charging times" that must be addressed before they include it again). Likewise, infrastructure adoption is unparalleled with Qi included in over 35 automotive models, IKEA furniture, Corian countertops, and standalone Qi transmitters of different shapes, colors, and sizes (to name only a few…).

AirFuel adoption is limited mostly to pilot scale. Dell launched a laptop in 2017; LG launched a limited-edition phone; and a variety of infrastructure deployments and accessories have pilot deployments in hotels, sports venues, airports, and coffee shops around Asia, Europe, and the U.S.

Proprietary NFMC has surprising levels of deployment, partially owed to the fact that certain niches have been using wireless power since the 90s. For example, implanted neurostimulators, electronic toothbrushes, and industrial equipment interconnects have been leveraging magnetic-coupling technology for over two decades. Granted, the technology has evolved to be much smaller, faster, and more user-friendly today, but millions of products have been shipping annually using proprietary near-field magnetic coupling since the early 2000s.

RF has no major commercial deployment, but has been impressively displayed by a variety of technology developers, including phone-charging demos where multiple phones are charged simultaneously at distances up to 15 feet away from the source. Most companies developing RF technology are in the pre-regulatory phase of development or have created off-shoot products that utilize RF technology, but at distances substantially lesser than the ultimate promise of RF.

Ultrasound is in the earliest stage of all. Limited demos have been provided, but no commercial products are available. The few demos offered are similar to RF demos in that they appear to slowly charge cell phones at distances of a few meters away from the source. The development efforts seem to be early stage and potentially still confronting fundamental challenges.

USE CASE

The main value of Qi is that it's interoperable and going to be everywhere. The main limitation of Qi is the use case. Qi relies on tightly coupled technology, low frequency, and limited in-band communication. For users, this means that device separation is limited to 3-5 mm, flexibility is limited, and the promise of simultaneous charging and data-transfer rate depends on an external data protocol.

There are workarounds for most of the limitations. For example, multiple-source power supplies and coil arrays can be used to provide greater orientation flexibility. The challenge, however, is cost of those complex systems and challenges with backwards compatibility. Over time, the technology and use case will improve. For now, this is the main shortcoming of Qi.

AirFuel Resonant's major promise is use case. AirFuel utilizes loosely coupled technology, which means that multiple devices can charge from a single transmit coil simultaneously; orientation and distance (up to ~50 mm) is flexible; power levels can scale reasonably above 50 W; and device charging can be invisible and more intuitive (i.e., embedding transmitters under the counter versus visibly embedding in or on the counter).

For AirFuel to succeed, it needs adoption and scale. Superior technology and use case may win over customers in the long term, but there's a significant uphill climb given Qi's current market leadership.

Proprietary NFMC has the most flexible use case because it's proprietary. Everything from multiple-device charging with high power and unique environmental constraints down to low-power, low-cost 1:1 systems with no data transfer is fair game.

RF provides an extremely compelling use case. Whereas Qi offers millimeters of separation and AirFuel offers centimeters of separation, RF offers meters of separation. To date, long-distance RF power transfer still isn't expected to deliver much more than 1 W of power, but it has the potential to be extremely valuable for low-power applications that rely on positional flexibility and meters of separation.

Ultrasound's use case is less well known due to the limited technical information available. Most likely, the use case is somewhat similar to RF's in that it has the potential to deliver low power over meters of distance.

SAFETY AND REGULATORY

Qi is implicitly safe due to magnetics and close-proximity coupling. It's achieved regulatory approval in all major con-

TECHNOLOGY READINESS				
Qi	AirFuel	Proprietary NFMC	RF	Ultrasound
In market and developing next-gen improvements	In pilots and early production	In market and developing breakthroughs in novel use cases	Demo and pre-regulatory stage for main products	Limited demos

sumer markets and has limited issues with interference due to low frequency (~200 kHz), minimal radiation, and known shielding techniques.

AirFuel is also implicitly safe for similar reasons to Qi, but is challenged a bit more on interference-related issues due to higher frequency of operation (6.78 MHz) and generally larger transmitter antennas (for orientation flexibility). Multiple AirFuel systems have achieved worldwide regulatory approval, but regulatory is not a “given” (EMI/EMC issues, not safety issues) and should be carefully designed.

Proprietary NFMC can’t receive a blanket statement because every system is unique. NFMC (the same type of physics used by Qi and AirFuel) is generally safe. Designers must carefully consider EMI/EMC for each proprietary product design.

RF over distance hasn’t achieved regulatory approval. The power required in the transmitter to deliver usable power to devices multiple meters away is significant. In other words, current systems will need to be improved in order to provide enough power with low-enough emissions and high-enough efficiency to pass regulatory muster. This is a significant challenge since power reduces exponentially as it radiates away from a source due to the inverse-square properties of EM waves.

Ultrasound technology at low power is safe, but can it deliver meaningful amounts of power at meters of distance? Again, laws of physics are stacked against ultrasound technology, and the technology is too early stage for meaningful data to be publicly available. However, proponents of this technology are surely working on developing breakthroughs. ed

JACOB BABCOCK is co-founder and CEO of NuCurrent, a leading wireless power system and magnetics solution provider. NuCurrent’s patented technology, proprietary tools, and design techniques mitigate typical high-frequency effects, offering higher efficiency, smaller sizes, higher durability, and lower total cost for wireless-power-system implementation.

Design Note

Cool Running, 144W, 4 × 40A µModule POL Regulator

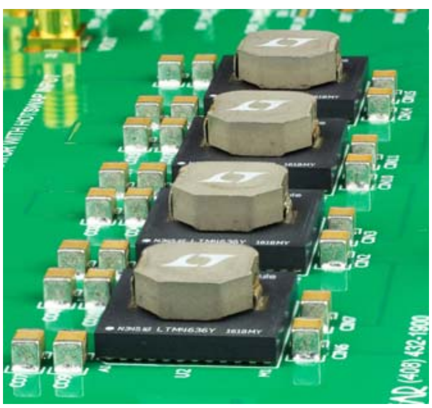
Afshin Odabaee and Yan Liang

Introduction

The LTM®4636 is a 40A-capable µModule® regulator featuring 3D packaging technology, or component-on-package (CoP) to keep it cool—see Figure 1. The body of the device is an overmolded 16mm × 16mm × 1.91mm BGA package with an inductor stacked on top to expose it to cooling airflow. The total package height is 7.16mm.

In addition to dissipating heat from the top through the exposed inductor, the LTM4636 efficiently disperses heat to the PCB via 144 BGA solder balls dedicated to GND, V_{IN} and V_{OUT}—where high current flows.

A single LTM4636 is rated for 40A loads; two parallel converters can support 80A; four support 160A. Upscaling a power supply by paralleling LTM4636s is easy: simply copy and paste the single-regulator footprint, as shown in Figure 1.



DN529 F01

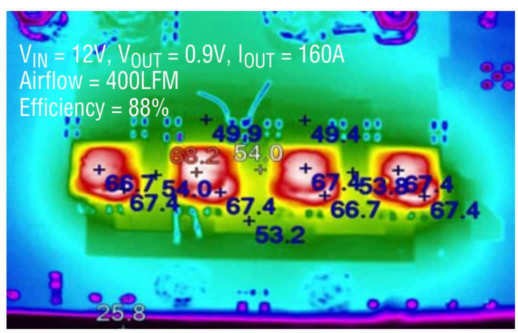
Figure 1. 3D Packaging of the LTM4636 Puts One of the Hottest Components, the Inductor, on Top, Where Significant Surface Area Is Exposed to Airflow. It Is Easy to Lay Out Parallel LTM4636s to Scale Power Capability—Simply Duplicate the Layout of One Channel and Multiply. The Clean Layout Here Shows Four Channels at 40A Each.

The current mode architecture of the LTM4636 enables precision current sharing among the 40A blocks. Precise current sharing, in turn, produces a power supply that spreads the heat evenly between devices. Figure 2 shows that all devices in the 4-µModule 160A regulator operate within 1°C of each other, ensuring that no individual device is overloaded or overheated. This greatly simplifies heat mitigation.

Figure 3 shows the complete 160A design. Note that no clock device is required for the LTM4636s to operate out-of-phase to each other—clocking and phase control is included. Multiphase operation reduces input and output ripple current, reducing the number of required input and output capacitors. Here, the four LTM4636s run 90° out-of-phase.

Conclusion

Choosing a POL regulator for a densely populated system requires scrutiny beyond voltage and amperage ratings of the device. Evaluation of package thermal characteristics is essential, as it determines the cost of cooling, the cost of the PCB and final product size.



DN529 F02

Figure 2. Precision Current Sharing Among Four LTM4636s Running in Parallel, Resulting in Only 40°C Rise in Temperature for 160A Application.

10/17/569

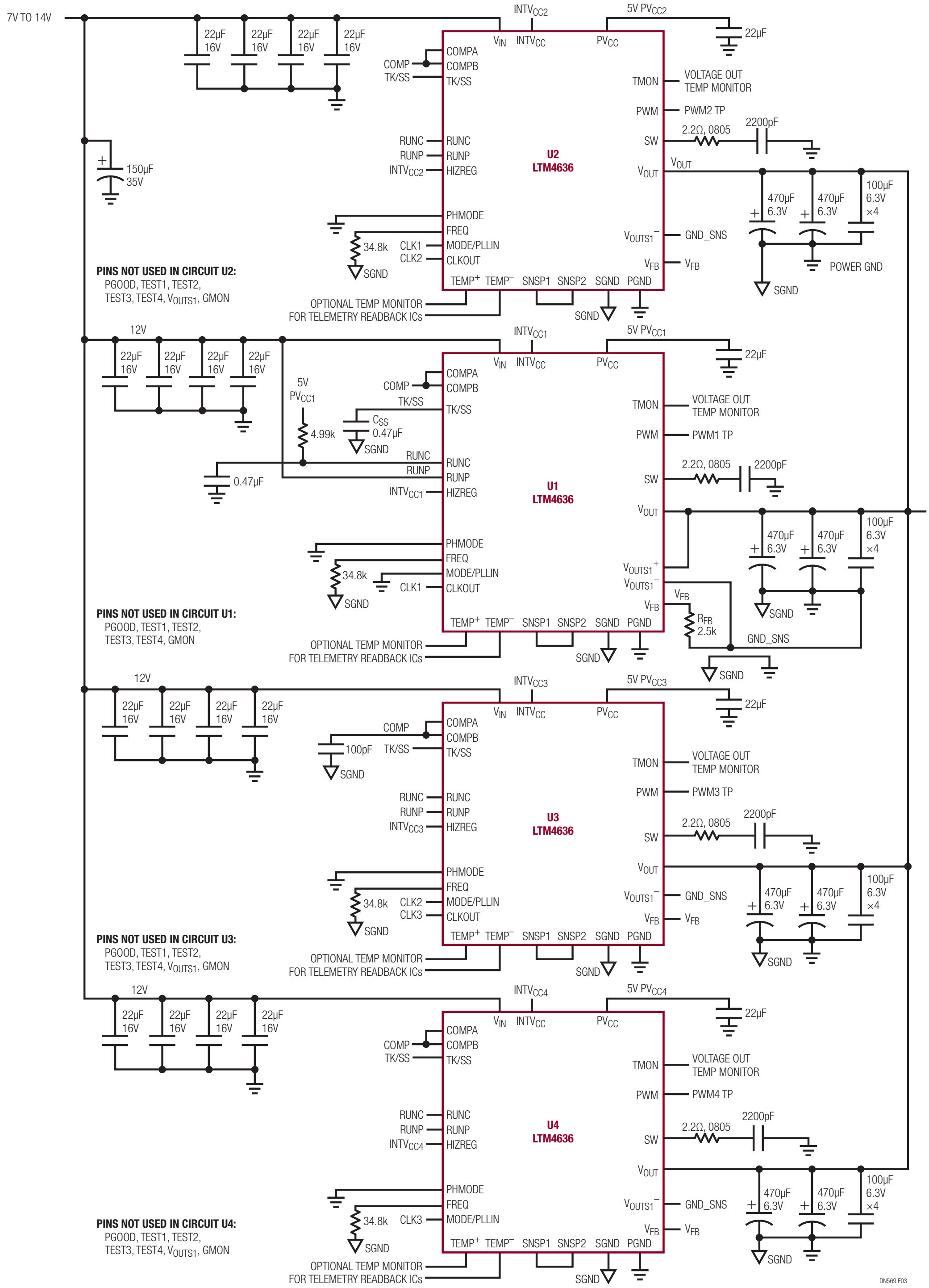


Figure 3. 140W Regulator Features Four LTM4636s Running in Parallel with Precision Current Sharing and High Efficiency 12V Input to 0.9V Output at 160A

Data Sheet Download
www.linear.com/LTM4636

For applications help, call (408) 432-1900

DN569 LT/AP 1017 305K • PRINTED IN THE USA

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™

CRYSTAL WARD KENT and BERNHARD MUEGGLER | CEO, swissRTec

The Future of Electronic Waste

Electronic waste is the fastest-growing form of waste. Could recycling be a new revenue stream and an environmental boon?

Japan is a small, island nation, but its efforts in electronic waste recycling are attracting international attention. Could the United States learn from the Japanese model? With a population of more than 127 million, Japan recycles more than 2 million tons of electronic waste annually. America only recycles about 679,000 tons annually, and that figure doesn't include a large portion of electronics such as televisions, DVD and VCR players, and related TV electronics, per the U.S. Environmental Protection Agency (EPA).

In the U.S., E-waste represents 2% of America's trash in landfills, but 70% of overall toxic waste. In fact, according to the EPA, E-waste is still the fastest growing municipal waste stream. Not only is electronic waste a major environmental problem, it contains valuable resources that could generate revenue and be used again. Cell phones and other electronic items contain high amounts of precious metals, such as gold and silver. Americans dump phones containing more than $60 million in gold and silver each year!

The Japanese model has also attracted the attention of Russia, as this nation seeks to launch more significant national recycling efforts. President Vladimir Putin is calling 2017 "The Year of Ecology," and has stated that improved recycling is a top priority. In fact, Russia hosted the 2nd Congress of Eurasian WEEE Solutions in Moscow this past March.

The Congress, which is part of the Moscow International Recycling Expo, is a platform where those in the Eurasian Economic Union (EAEU) are able to discuss opportunities, solutions, and challenges within the recycling industry, as well as network and develop relationships with recyclers, producers, scientists, regulators, and municipalities, among others key to the industry. The EAEU, which is comprised of the Russian Federation, Belarus, Kazakhstan, Kyrgyzstan, and Armenia, is one of the fastest-growing recycling markets, generating more than 1,500,000 tons of WEEE annually.

Given Japan's success, and key interest by nations such as Russia, might it not be time for the U.S. to consider other options when it comes to E-waste?

Not only is electronic waste a major environmental problem, it contains valuable resources that could generate revenue and be used again. Cell phones and other electronic items contain high amounts of precious metals, such as gold and silver.

HOW THE JAPANESE MODEL WORKS

In Japan, the electronic waste comes from a number of sources. East Asia is major consumer of electronics and electric appliances, so with each upgrade, millions of outdated models are discarded on a yearly basis. The region also controls a major global share of the import and export of these same products. In addition, trade in electronic waste has been booming in recent years. All of these waste streams combined have raised questions about their potential environmental impacts, and it is these concerns that led Japan to take some significant steps in addressing the issue—and much sooner than most other developed nations.

Japan had already begun to look at the big picture, in terms of electronic waste disposal, back in the early 1990s when they became the first country to enact a law specifically concerning electronic waste. Four factors were behind this legislation:

1. Recognition of the difficulty of disposing of electronic waste compared to other kinds of waste.
2. A major shortage of landfill sites, and concerns about the contamination of soil, groundwater, and other resources.
3. Growing awareness of the benefits of recovering and utilizing the valuable resources contained in electronic waste.
4. The willingness to develop recycling companies as a "venous industry," a Japanese term for businesses that turn solid industrial waste back into raw materials that can then be used anew.

The ground-breaking Home Appliance Recycling Law went into effect in 1991, and was designed to specifically help control the illegal dumping of items such as televisions, refrigerators, air conditioners, and washing machines. It addressed electronic waste on a number of fronts.

First, the law identified key products that could be targeted for mandatory recycling, such as those which were difficult for local governments to recycle, as well as those containing significant quantities of recyclable resources (e.g., metals) that are inexpensive to recover. It also noted products that could be easily recycled by consumers if they returned them to retailers upon the purchase of replacements. In addition, the law focused on products that could be made more recyclable with certain design modifications.

In 2000, Japan expanded its recycling mandates with the Basic Act on Establishing a Sound Material-Cycle Society, and the addition of its "manifest system." This system seamlessly tracks waste from the time it leaves the facility where it was produced until it reaches an off-site waste-management facility. At this time, no other country has such a "cradle to grave" tracking system. Not only does this system ensure that materials aren't disposed of wastefully or illegally, it also clearly outlines the responsibilities of all stakeholders involved in each part of the process.

The role of the consumer, in terms of their recycling responsibilities and how they cooperate with retailers and local governments, is clearly defined as well. Japan has different laws for different products, with some requiring compulsory recycling and others falling under voluntary initiatives.

In recent years, additional laws have continued to refine Japan's recycling efforts and give them a strong legal mechanism for enforcing the recycling of electronic waste. In addition to the aforementioned products, personal computers and mobile phones are marked for recycling. All of these products combined make up 40% of Japan's electronic waste.

Japan was also one of the first countries worldwide to implement an Extended Producer Responsibility-based system for electronic waste. This has been modeled on its solid-waste-management system, and has an advanced take-back system and processing infrastructure.

Given the extent of government regulation regarding the recycling of electronic waste, it's interesting to note that Japan's rules don't encompass the process of acquiring a recycling facility or how the recycling is done. Manufacturers can hire anyone they want to build the facility, select the equipment and technology they prefer, and process the waste as they see fit. The only government requirement they must meet is the amount of utilization required from each material that comes into their facility. Manufacturers often want to recycle in the least expensive way possible, which can be less efficient and result in less useful or valuable end products. Japan's regulations ensure that recycling yields the best possible results.

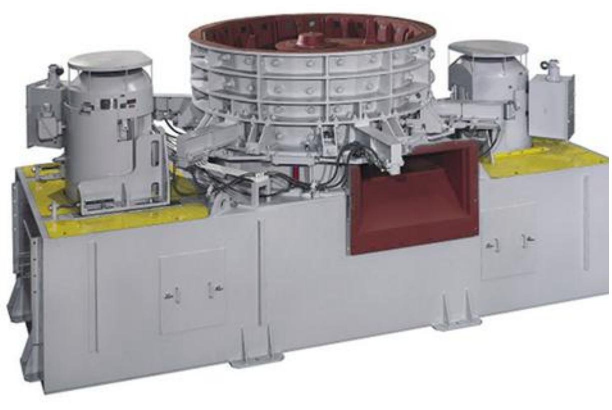
Currently, local governments collect electronic waste not subject to replacement purchase from consumers and transport these materials to collection centers run by the producers. Depending on the items purchased, and the circumstances, consumers may also pay retailers to pick items up—if the consumer has purchased a replacement item, then the retailer automatically picks up the older item. Consumers help bear the burden of recycling costs via fees that are levied on goods as they're turned in for recycling. Retailers and distributors also pay fees.

In 2001, Japan implemented the Law for the Promotion of Effective Utilization of Resources, which requires manufacturers to recycle goods and reduce the generation of waste.

According to the Association for Electric Home Appliances (AEHA), as a result of these laws and regulations, in 2013, 556,000 tons of electronic waste were officially collected and treated in Japan—that's roughly 24% of the electronic waste generated for that year.

TECHNOLOGY PLAYS A VITAL ROLE

The advent of sophisticated recycling technology has played a major role in the success of Japan's electronic-waste recycling program. Japan has approximately 100 major electronic waste facilities, as well as numerous smaller, local collection and operating facilities. Out of the 100 major plants, more than 30 utilize the Kubota Vertical Shredder to reduce the size of the electronic waste. With the Vertical Shredder holding roughly 30% of the market share, it's clearly the preferred choice of electronic-waste operators. In fact, Kubota has long dominated the Japanese market, and has been selling this shredding technology to the recycling industry for more than 40 years.



The Kubota vertical shredder is efficient, compact, and does pre-shredding and secondary shredding in a single pass.

The mighty Kubota Vertical Shredder can process large and small domestic appliances, metal scrap, and other bulky items, thanks to some unique features that make it indispensable to the recycling industry. It breaks down and grinds up materials down to one inch or less in size in a single pass, and the particle size can easily be adjusted.

The Vertical Shredder can be used as a standalone unit or in combination with other processing technology, which tends to be the most popular option. Close to 400 users have already taken advantage of its powerful breakers and multiple layers of grinders to process a broad variety of waste materials.

swissRTec of Switzerland is a frequent distributor of the Kubota Vertical Shredder technology. The company is a leader in designing, building and commissioning turnkey e-waste, scrap-metal, and ASR (automotive shredder residue) recycling facilities. The company's core focus is the shredding, delamination, and separation of valuable raw waste materials from waste compound materials.

"More than 40 years of proven technology are built into the Kubota Vertical Shredder," says Mario Zoellig, CEO of swissRtec. "It is efficient, compact, and does pre-shredding and secondary shredding in a single pass. Output particle size can be as small as one-quarter inch when processing ASR. Most important, choke rings allow for adjustment of particle size—no screens are required. It is designed for continuous operation, is versatile, and very efficient to operate."

The Kubota Vertical Shredder comes in various models, sizes, and power options to fit the diverse needs of recycling customers, and works well in combination with the swissRTec Delamination Mill. The Delamination Mill is an "impact mill" that uses thousands of collisions to break down pre-shredded composite materials, isolate various components, and then mill them into tiny, smooth balls that are easily separated.

Without such technology, recycling on a large scale, such as that embarked on by Japan and contemplated by Russia, would not be possible or profitable. With efficient recycling systems, for every one million cell phones that are recycled, 35,274 pounds of copper, 772 pounds of silver, 75 pounds of gold, and 33 pounds of palladium are recovered.

"The technology available with the Kubota Vertical Shredder and the swissRTec Delamination Mill meets the operating needs of today's companies," says Zoellig. "The shredder provides optimal flexibility for serving various industries, and that, combined with the fine processing capabilities of our Delamination Mill, allows companies to process waste more efficiently. When you recycle, you cannot control your intake—you have to deal with the materials that come your way. But our shredder allows you to better adapt to what comes in, and thus make processing more productive and economical."

Whether Russia follows Japan's lead and issues government mandates regarding the recycling of electronic waste, or relies on privatization and entrepreneurship to grow their recycling industry, one thing is clear: Recycling of electronic waste is essential as the problem will only expand not diminish. The bright spot is that with the right technology, it can also be quite lucrative, create essential jobs, and generate new revenue streams. ed

BILL BOLDT | Business Development Manager, BlackBerry

AUTOMOTIVE SECURITY in a CAN

With car safety issues extrapolating due to the rapid increase in electronics, the automotive security market has been forced to immediately transition from effectively no security to robust security implementations.

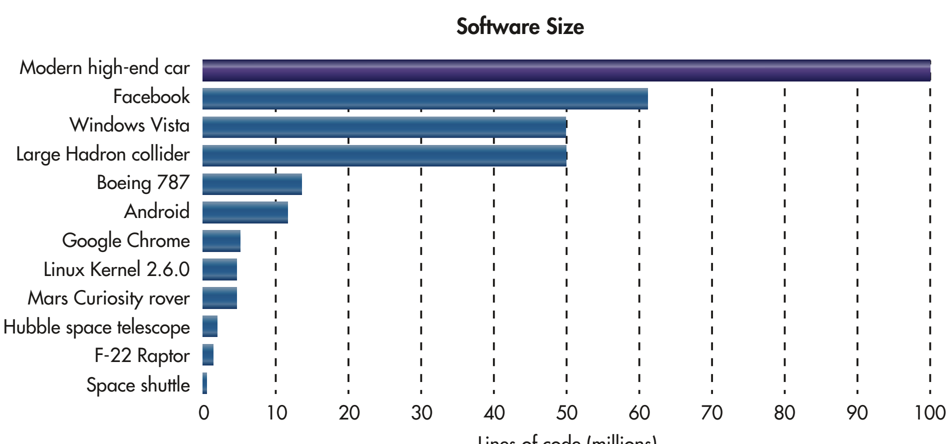
The automotive security market is at a clear inflection point—safety issues are forcing the industry to move from effectively no security to robust security implementations almost instantaneously. Many powerful market drivers and fast changing dynamics are putting security into the driver seat, especially when the driver isn't a human.

When any embedded system, especially a vehicle, becomes connected, the first thought should be "how secure is it?" For connected vehicles, until recently, security has been an afterthought at best. That fortunately is changing, which is important because vehicles are becoming largely defined by software as they evolve toward connected autonomous drive.

As entrepreneur and software engineer Marc Andreessen famously said, "Software is eating the world." If that is true, the next course will be served on wheels. It should be clear to any observer by now that software is already becoming the basis of automotive competition for automakers. Statistics show that software will become the main driver of an automaker's profitability.

Autonomous driving, connectivity, and other initiatives are making automotive software highly complex with more lines of code than a sophisticated fly-by-wire jet fighter. Connectivity and large code size make vehicles more vulnerable to hacking, raising safety issues. In fact, the industry was given some high profile wakeup calls over the last few years.

Hacks of automotive buses and electronic control units (ECUs), most notably by Dr. Charlie Miller and Chris Valasek of the Jeep, undeniably illustrate that robust cryptographic security is needed, and quickly. That's due to the simple calculus in the increasingly software-based connected vehicle (and smart highway infrastructure)—without robust cryptographic security, there cannot be safety *(Fig. 1)*. Security will become the table stakes for any new automotive design, right down to the specific processors. Security must become endemic to automotive systems and subsystems just like DNA is to an organism.



Source: NASA, IEEE, Wired, Boeing, Microsoft, Linux Foundation, Ohioh

1. This chart depicts software size, representing millions lines of code required for each application.

INSECURITY MEANS LIABILITY

The market for automotive security is driven by the fact that current control systems in cars (such as ECUs operating over control-area-network, or CAN, buses) are insecure, which exposes automakers to enormous potential liability. Such liability can only be addressed with technology that's more advanced than that of the attackers. Because of the high-profile hacks, the deep pockets of carmakers, and the "win the lottery" nature of such litigation, the race to secure vehicles has started. However, car-makers are in catch up mode.

It may not be long before the commercials for asbestos poisoning are replaced with actions for injuries stemming from insecure vehicle systems. If you think about it, in a human-driven car, the human is responsible. In a car driven by software systems, though, it's very likely that the maker of the car will be held responsible.

Automotive safety and security risks have already attracted the attention of legislators in Washington D.C., and if the history of legislating the automotive industry is any clue, there's much more to come. Because public safety is at stake with automotive hacking, specific cryptographic security will increasingly be mandated by legislation. However, the specifics aren't clear.

The most salient examples of legislative interest in automotive security is the Markey Car Security Report and the SPY Car Act. With Washington getting into the act, clearly there will be increasing urgency to design, analyze, test, respond, and standardize automotive security. However, before technical solutions can be standardized and/or legislated, it's critical to understand what is meant by "automotive security."

THE MOBILE COMPUTE-PLATFORM

The connected autonomous car will morph into a sophisticated networked compute-platform, integrated with fused sensors and actuators, and be increasingly controlled by artificial intelligence. This is becoming clear by now.

Vehicles are already a hybrid mechanical-electrical control system with a wide range of ECUs sending and receiving signals over evolving signaling buses to act in a coordinated, organic way. ECUs are controlled by increasingly sophisticated and complex software. But, for connected, networked cars to be safe, the software and hardware must be extremely secure, meaning they must have multi-layered robust cryptographic security mechanisms built right in.

Cryptographic security means that mathematical algorithms, methods, protocols, cryptographic keys, and certificates like those used to secure banking systems, smart cards, mobile infrastructure, and secure websites must be designed into vehicles (and into their manufacturing systems). These methodologies will be used to protect sensors, actuators, ECUs, communications buses, ECU access points, and gateways to the outside world.

Today, signaling buses and ECUs aren't very secure and a hacker can inject malicious messages to make a car potentially unsafe. One might even say that without security, the notion of a connected autonomous car can't be safely realized. No safety means no connected autonomous car industry.

If autonomous cars are the next big thing, then a truly robust automotive security architecture for ECUs, gateways, domain/area controllers, and their manufacturing systems is the thing that makes the next big thing possible. Therefore, it's not an overstatement to say that robust cryptographic security is the sine qua non of the automotive future.

ECUs are at the heart of the automotive security challenge because they and the buses that connect them need to be secured. There's no way to tell if the signals or messages sent are from an authentic sender, or if they have been corrupted (i.e., have lost data integrity). That must change quickly, and every carmaker, ECU producer, and automotive semiconductor supplier knows it and is working on it. However, there are no standards and these approaches often tend to be fragmented.

ECUs are little computers that run a wide range of systems, including the powertrain; things inside the car like seats, mirrors, windows; multimedia systems; braking systems; safety systems (e.g., airbags); emerging assisted driving mechanisms; and sensor/actuator platforms, among others. Because ECUs control remote systems, they need to be connected to those things (obviously), and that's done over various types of buses such as CAN, LIN, FlexRay, MOST, and others. Eventually, as more data is gathered and processed by cars, higher bandwidth networks like to those now used by PCs (e.g., Ethernet) will be widely employed. This shift has started.

As for security, as the number of computing nodes in a car network grows, the ways in which these nodes can be attacked increases exponentially (some experts say to the 4th exponent of the number of nodes).

Automotive cryptographic standards and architectures for secure ECUs and other processors aren't standardized. OEMs, Tier Ones, and Tier Two semiconductor suppliers haven't agreed on a common standard for securing and updating vehicles and factories, but are looking to each other for a holistic solution that none currently can offer. Past standardization activities such as the European Union's EVITA and the Hersteller Institute of Software's Secure Hardware Extension (SHE) are still in their infancy despite nearly a decade of work by important parties in the automotive ecosystem.

What this means is the clay is wet when it comes to automotive security, and many proposals are being made by startups, established computer security companies, networking companies, management consultants, IP providers, mobile communications companies, OEMs, Tier Ones, Tier Twos, and others.

Given the cat-and-mouse nature of digital security, and the accelerating advances in connected autonomous vehicle technologies, there will always be a certain amount of cryptographic evolution and flux, making the task to define and standardize architectures challenging. The ability to adapt to the unknown must be built into any security solution. That point can't be emphasized enough.

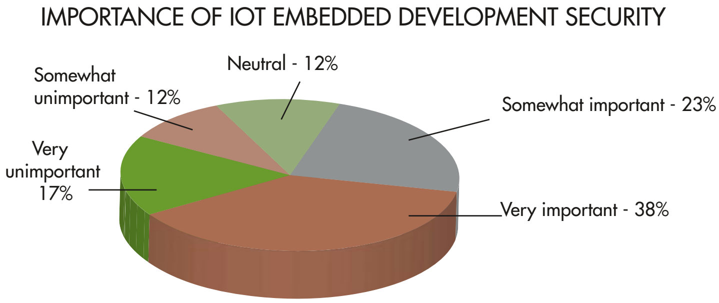
PRINCIPLES OF AUTOMOTIVE SECURITY

Despite uncertainties and changing market dynamics, some automotive security principles are starting come into clear focus:

- Automotive security begins with the semiconductor processor. These processors need to be personalized using private keys injected by secure equipment and processes. Certicom's Asset Management System is an example of equipment used to accomplish this task.
- The next step is to ensure that the operating system is secure. An example is the microkernel-based architecture of the BlackBerry QNX SDP 7.0 OS. It separates critical OS components into their own protected memory partitions, provides temporal separation for threads, uses an encrypted file system, offers multi-policy driven security features, and provides network security to reduce the attack surface.
- Different levels of safety criticality must be managed. An example of that is the BlackBerry QNX true Type 1 hypervisor, which allows isolation between virtual functional modules, providing another layer of security and safety—it can isolate safety-critical from non-safety-critical functions.
- ECUs and modules will have certificates installed, which can be used to authenticate other modules, or other cars and infrastructure (i.e., V2X). These certificates must be issued and managed using a secure managed PKI system, such as offered by Certicom.
- Software must be readily updatable at dealers and repair shops, via secure over-the-air software update systems such as offered by BlackBerry IoT.
- Aftermarket suppliers must be able to sell and update the software on secure devices.
- Communication between ECUs must be authenticated and messages need to be signed to avoid rogue messages which can create havoc.
- Access to sensitive electronics of the car via different access ports needs to be protected against unauthenticated access.
- OEMs must be able to authorize or not authorize specific electronic devices at manufacturing time and after the car is in use (for example to enforce warrantee policies).
- Software needs to be scanned and validated for being secure. This requires very special tools, also provided by BlackBerry.

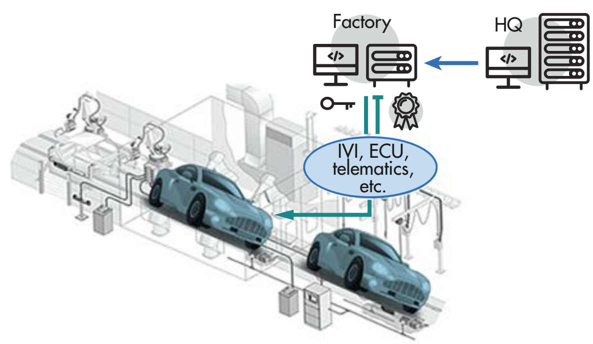
WHO'S IN THE LEAD NOW?

Interestingly, the recent results from *Electronic Design's* "Embedded Revolution" survey for IoT security *(Fig. 2)* match very closely with 2015 surveys focused on automotive embedded security, which was before the Miller-Valasek Jeep hack. Things have changed drastically since then.



2. Results from *Electronic Design's* Embedded Revolution survey on IoT security from a couple of years ago.

Primary research recently conducted with automotive OEMS, Tier Ones, and Tier Twos shows that the security is "Very Important" to well over 95% of the respondents. This new statistic indeed matches the evidence of large-scale investments being made into automotive security gateways, hardened ECU (hardware security modules, or HSMs) and domain controllers, secure manufacturing, secure operating systems, secure firmware over-the-air (FOTA) updates, security health monitoring, and secure processors *(Fig. 3)*. The automotive industry quickly went from being just like any another embedded application when it came to security to being the clear frontrunner with a profound sense of urgency.



3. Many precautions and technologies need to be interwoven into system development because security is a multifaceted and multilayered proposition.

SECURITY STARTS IN THE SUPPLY CHAIN

As noted above, security mechanisms such as keys and certificates must be injected into ECUs in the factory and in the field. To do this, a secure manufacturing system must have global reach, be manageable on a distributed basis, be updatable by various entities, and remain secure for years. To maintain the maximum amount of flexibility, personalization and updating should be moved as close as possible to the very point in production, which is a critical objective of the global manufacturing blueprint *(Fig. 4)*.

MULTI-LEVEL SECURITY

With cars, security must happen on multiple levels. Multi-level cybersecurity will not be an option, but will be commercially mandatory and mandated by the government *(Fig. 5)*. The signs are already there.

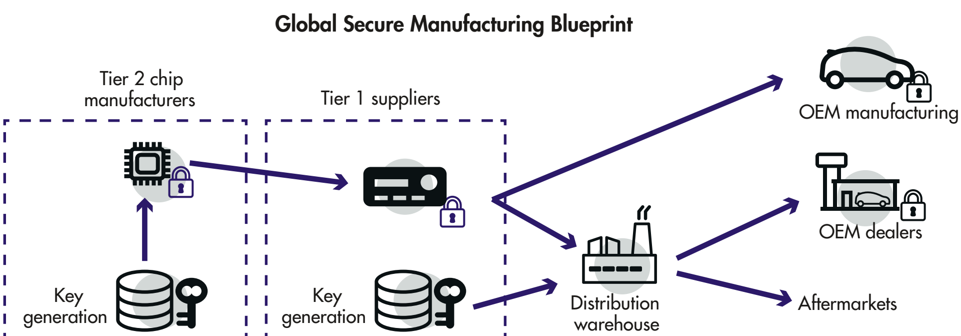
Multi-layered automotive security will likely include a mix of the following items *(Source: NXP, Argus, Roland Berger, IHS, Strategy Analytics, ST Micro, Infineon, Bosch, Elektrobit, Microchip, Renesas, Harman, Deloitte, PwC, McKinsey & Co., Intel, IO Active, Automotive OEMs, BlackBerry QNX, Certicom, others)*:

- Isolating in-vehicle electronics from external interfaces by means of firewalls.
- Applying strict access control to only allow known/trusted entities (partial) access to in-vehicle systems.
- Clustering in-vehicle networks with similar criticality into domains to better isolate safety-critical systems from others.
- Protecting in-vehicle networks with cryptographic authentication, data integrity, and maybe perhaps later encryption.
- Using intrusion detection/prevention systems (IPS/IDS) to detect and counter attacks.
- Protecting ECU operation via secure boot, secure update, and others.
- Upgrading ECUs to include secure processors.
- Secure gateways, transceivers, and switches to protect networks.
- Protecting cryptographic keys using hardware-based key storage (e.g., secure crypto elements and/or HSMs).
- Using high-speed secure crypto elements to authenticate V2X signals.
- Movement toward PKI-based security using a hardware root of trust and active certificate management.

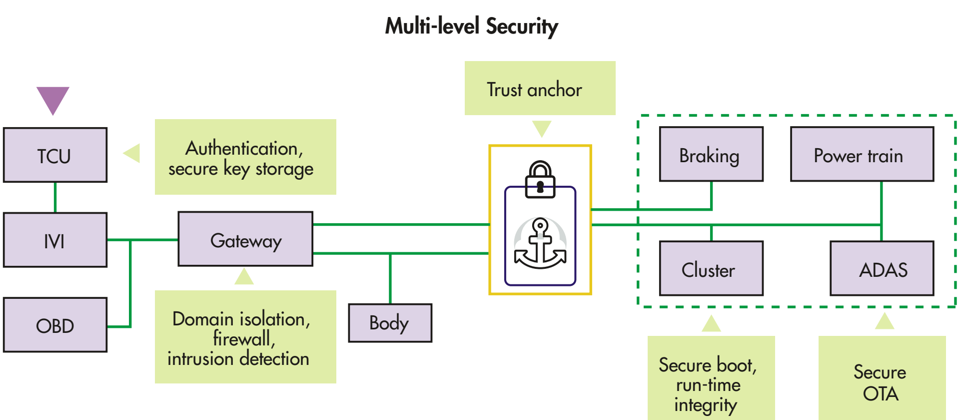
PLAYING CATCH UP

CAN bus insecurity coupled with high-profile hacks has put carmakers into a position where they're playing catch up. With cars being connected and with the growing code base, vulnerabilities are growing. This creates what's referred to as an expanding attack surface. Simply put, cars are hackable in an increasing variety of ways *(Fig. 6)*.

Exposure to attacks is now well-known; thus, the industry must quickly find ways to cryptographically secure existing low-bandwidth buses such as CAN and the ECUs that connect over those buses. Higher-bandwidth buses like Ethernet are coming to automotive platforms to address the need for faster and higher volumes of information. These systems will have stronger security mechanisms, but they're not coming in time to obviate the need to retrofit the existing CAN bus for robust security. That's a core issue, and it presents almost overwhelming challenges when it comes to resource, cost, implementation, and management (especially of security keys).



4. Shown is one sample of a global secure manufacturing blueprint.



5. Multi-level cybersecurity will no longer be an option. Rather, it will be commercially mandatory and mandated by the government. *(Source: NXP)*

SO, WHERE ARE WE?

The automotive security industry, as noted, is in its infancy. There are no clear technological winners yet regarding the type of security that will be adopted for cars and smart infrastructure. Shared RSA keys, RSA-based PKI, ECC-based PKI, and mixed systems are all in various states of exploration and implementation with OEMs, Tier Ones, and Tier Twos. Different types of key storage and updating are being used and contemplated, including automotive trusted platform modules (TPMs), HSMs, and other methods.

The evolution of security techniques is happening on a purely pragmatic basis because standards don't exist and may not for a while. The industry is taking a crawl-walk-run approach, which means that some type of quick-to-implement security solution, perhaps using shared symmetric keys, appears to be an emerging first step (crawl). That may be followed by a more robust approach using public key infrastructure (walk). Subsequently, an even more secure approach using higher bandwidth buses like Ethernet and more sophisticated domain/area controllers and gateways equipped with PKI-based solutions may be adopted (run).

PKI is highly likely to be a part of any long-term solution. That's because PKI is more secure and manageable at finer resolution (i.e., a key for each ECU) than shared key approaches.

Security is required not only on the control buses and ECUs, but also on vehicle-to-vehicle and vehicle-to-infrastructure (collectively V2X), as well as on manufacturing and updating systems. Different schemes will be implemented for V2X and internal vehicle security due to differing needs. V2X is already adopting PKI.

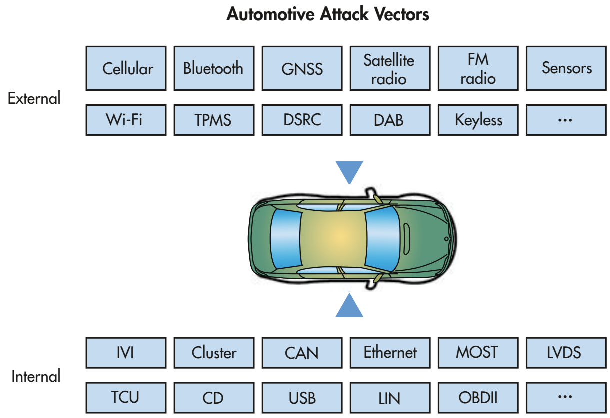
FINAL THOUGHTS

A critical dynamic worth paying attention to in the automotive industry today is a shift in terms of who will control software development, including security. OEMs recognize that they must be in control of automotive software development because security and safety are interlinked and must be built into the foundation of the design into every layer.

Many refer to the dynamic of connected, autonomous, software-driven cars as Silicon Valley invading Detroit (at least in American parlance). "Detroit" is responding by becoming more software savvy, which means hiring, acquiring, and partnering on software, from operating systems, to artificial intelligence, to cryptography, and over-the-air software updating.

Just as automakers are taking more responsibility for software development, silicon makers are taking more responsibility for system definition. They're adopting more risk to get ahead of the curve and provide the silicon and increasingly the software that runs on the silicon. They can't do it alone, so they're partnering with software companies skilled in the art of automotive security and safety.

Due to the long semiconductor design cycles, especially for multicore processor-based products, and the long automotive design cycles, semiconductor companies must anticipate market needs more than ever, and well before standards are set and requirements codified. Multicore processors with complex graphical processor units (GPUs) are expensive to design. Despite the increasing levels of risk, there is a silicon land grab underway, and the spoils will likely go to the most innovative and daring companies.



6. There are multiple ways to hack a car.

Due to the need to provide security under time pressure from the threat of liability and regulation, semiconductor companies making automotive processors simply have no choice but to propose advanced security solutions, with the risk that some of these may never get adopted or standardized.

Evidence of the semiconductor companies' technical and market leadership include automotive hardware security devices of various flavors such as HSMs, secure processors, and automotive TPMs. One thing common to these devices is that silicon makers have figured out that the key to cryptographic security is keeping the secret key secret. Therefore, these products are increasingly storing the secret key in secure hardware. Think of that as a secure key vault.

Of course, the other side of the silicon equation is software. Silicon and software should work together intimately and securely if vehicles are going to be safe. Software needs secure hardware, which must be made and updated on secure equipment. Knowing this, it's already possible to decrypt the software-defined automotive future: Silicon, software, safety, and security must become seamless. ed

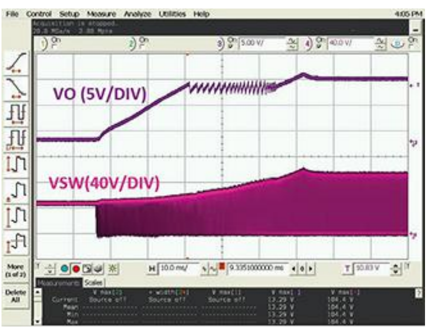
BILL BOLDT, business development manager at BlackBerry, is responsible for security-related products. He's held various marketing and business development roles at Atmel, Fairchild, TDK, and Silicon Systems, and ran an industrial design firm. Bill has spoken about and published numerous articles on security, semiconductors, and technology markets. He holds a BSEE from the University of Notre Dame and Masters in management from Kellogg (Northwestern).

Circuit Ensures Smooth "Soft Start" for Isolated Converter, Limits In-Rush Current

By MANJING XIE | Texas Instruments

MOST DC-DC CONVERTERS require a soft-start circuit to limit the in-rush current at startup. Although a smooth soft start is required for systems with power-on reset (POR), this is difficult to implement in an isolated converter with a controller on the primary side and a limited duty cycle or current.

Figure 1 shows the soft start of a forward converter with a duty-cycle soft start from the primary side. The steady-state output of the converter is 12 V. A 50% load current is applied at 10 V, which is the POR threshold of the system. As soon as a load is applied, the output drops and triggers system shutdown, causing the system power to cycle several times. At the end of soft start, the output overshoots 10%, which is not desirable.

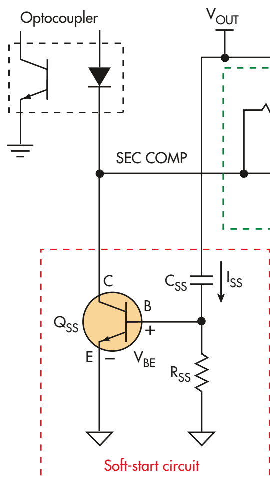


1. The output of a forward converter during startup mode, with a load applied at 10 V, shows the system power-cycling and the output overshooting by about 10%.

A simple circuit can implement a smooth soft start for an isolated converter in a system using the LM5025 active-clamp, voltage-mode PWM controller. *Figure 2* shows the concept of this secondary-side soft-start approach.

When first applying the input, the converter output (V_{OUT}) starts to rise, capacitor C_{SS} is charging up, and the C_{SS} charging current (I_{SS}) flows through resistor R_{SS}. When I_{SS} is higher than $V_{BE(on)}/R_{SS}$, Q_{SS} then turns on and starts to pull current from the secondary-side comp node (SEC COMP), thus reducing the duty cycle. During soft start, the error amplifier saturates and the soft-start circuit dominates the feedback loop. The converter, C_{SS}, R_{SS}, Q_{SS}, and optocoupler form a closed loop. When the output rises to regulation, the error amplifier starts to regulate and I_{SS} goes down, thus turning Q_{SS} off.

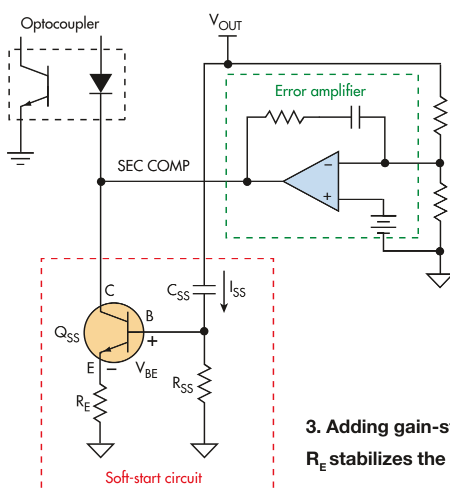
Equation 1 shows the transfer function from V_{OUT} to the optocoupler current:



2. The basic secondary-side soft-start approach adds an auxiliary circuit to the secondary-side compensation node.

$$G_{SS}(s) = \frac{i_D(s)}{v_{OUT}(s)} = \beta \cdot C_{SS} \cdot s \qquad (1)$$

While effective, this simple circuit might not be stable because the Q_{SS} forward gain β is high and varies dramatically from part to part. To stabilize this circuit, you need to insert a gain-reducing resistor R_E between the emitter of Q_{SS} and ground *(Fig. 3)*. Increasing R_E can reduce the feedback-loop gain during startup.



3. Adding gain-stabilizing resistor R_E stabilizes the soft-start circuit.

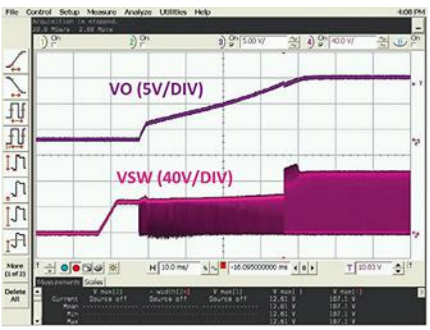
Equation 2 shows the soft-start circuit transfer function with R_E:

$$G_{SS}(s) = \frac{\beta \cdot R_{SS} \cdot C_{SS} \cdot s}{(R_{SS} + \beta \cdot R_E) \cdot \left(1 + \frac{\beta \cdot R_E \cdot R_{SS} \cdot C_{SS} \cdot s}{R_{SS} + \beta \cdot R_E}\right)} \quad (2)$$

At high frequencies, Equation 3 is an approximation of Equation 2:

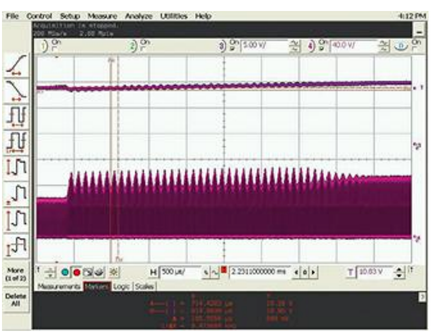
$$G_{SS}(s) \approx \frac{1}{R_E} \quad (3)$$

For testing, the soft-start circuit to the converter was set up with C_{SS} = 0.1 µF, R_{SS} = 100 kΩ, and R_E = 1.18 kΩ. *Figure 4* shows the soft-start waveform with these circuit parameters. When the system starts pulling current, the soft-start circuit stops drawing current from the COMP and the duty cycle increases quickly. The converter continues to soft start after a minor dip caused by the load transient.



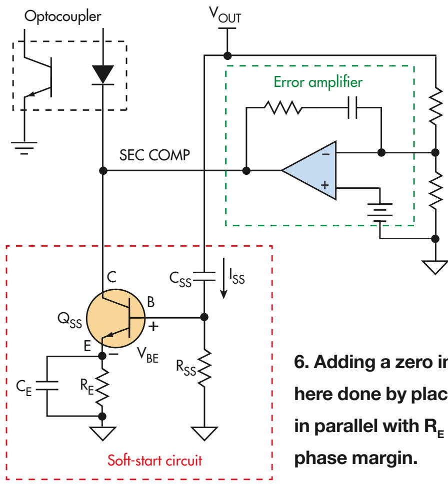
4. The soft-start waveform shows the circuit stops drawing current from the COMP pin; as a result, the duty cycle increases and the converter continues the soft-start process.

The figure also shows that after the load is applied, the converter switching node (VSW) has an additional voltage spike. *Figure 5* shows the zoomed-in waveform, which reveals that the system oscillates at 9.5 kHz.



5. The zoomed-in soft-start waveform shows system oscillation at 9.5 kHz, which isn't acceptable.

The controller in this design is a voltage-mode controller. The power stage has 180° of phase drop because of the double poles. It's necessary to add a zero to improve stability, done by adding capacitor C_E in parallel with R_E *(Fig. 6)*. In order to add 45° to the phase margin, a zero was placed at 9.5 kHz (the measured oscillation frequency). With R_E = 1.18 kΩ, this required a 15-nF capacitor.

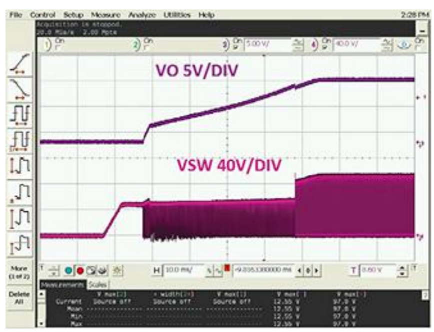


6. Adding a zero improves stability, here done by placing capacitor C_E in parallel with R_E to add 45° to the phase margin.

Equation 4 shows the soft-start circuit transfer function with R_E and C_E in parallel:

$$G_{SS}(s) \approx \frac{R_E \cdot C_E \cdot s + 1}{R_E} \quad (4)$$

Figure 7 shows the startup waveform with C_E = 15 nF. Note that the oscillation is eliminated, while the total soft-start time is 50 ms.



7. Adding the zero via the small additional capacitance eliminates the oscillation; the final circuit has an overall soft-start time of 50 ms.

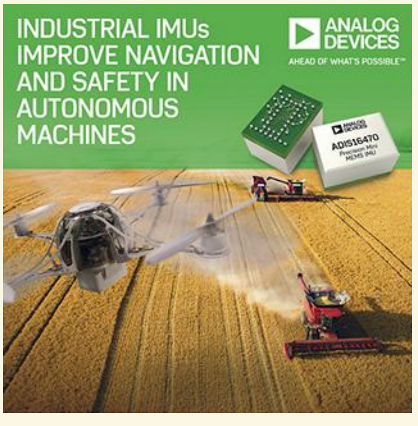
During soft start, the typical optocoupler diode current (I_{opto_D}) is between 1.2 and 0.8 mA, which is determined by the LM5025 and the optocoupler forward gain. With R_E = 1.18 kΩ, the voltage across R_{SS} is $V_{BE(ON)} + R_E \times 0.8$ mA = 1.644 V. Since $V_{BE(on)}$ = 0.7 V, you can calculate I_{SS} as $I_{SS} = (V_{BE(ON)} + R_E \times I_{opto\_D})/R_{SS}$. I_{SS}/C_{SS} sets the output V_{OUT}, dv/dt. To ensure the effectiveness of the secondary-side soft start, the primary-side soft start should be set to be much faster than the secondary-side soft start.

MANJING XIE is a power-system application engineer in the Power Design Services group at Texas Instruments. Manjing has more than 10 years of experience in ac-dc and dc-dc power-supply design and power-semiconductor development experience. Manjing received a BSEE from Tsinghua University and a MSEE from Virginia Tech.

Rugged COM Express Achieves SIL 2 Certification

MEN MICRO'S NEW CB30C Rugged COM Express module features a robust design particularly suited for safety-critical applications in rail or bus transport, and in industrial applications. EN50155 compliant, the product also meets EN50218 and EN50129 standards for software, system, and hardware development in railways, and is certified to safety integrity level SIL 2 with appropriate certification package, including safety case and certification report from TÜV SÜD. To achieve SIL 2 level, the board is monitored by a specially developed CPLD supervisor. If defined operating conditions like supply voltage or temperature reach critical limits, the safe supervisor interrupts power to the subsystem, ensuring all external communications are stopped. According to the RCE standard, the module operates from -40°C to +85°C via conduction cooling and is embedded in a solid aluminum frame protecting against environmental impacts like humidity, dust or electromagnetic radiation.

MEN MICRO, *www.menmicro.com*



IMUs Improve Navigation in Autonomous Machines

ANALOG DEVICES IS featuring a new series of five high-performance IMUs. The ADIS16470, ADIS16475 and ADIS16477 IMUs provide performance improvements that address the navigation- and safety-related needs of industrial applications in compact size with standard SMT assembly. The ADIS16465 and ADIS16467 IMUs offer similar performance advantages in a more ruggedized enclosure option. All of the IMUs provide six DoF sensing via triple-axis MEMS-based accelerometers and gyroscopes, and are focused on the demands of the IIoMT and its need for precise geolocation. Their performance allows systems to characterize motion accurately despite turbulence, vibration, wind, temperature, and other environmental disturbances, resulting in more-accurate navigation and guidance, and/or instrument stabilization. The IMUs are specifically designed to reject what are otherwise significant error sources, such as 'g'-influence, cross-axis sensitivity, and temperature and mechanical stress related drifts.

ANALOG DEVICES, *www.analog.com*

Power Meter Designed for Single-Phase AC Supplies

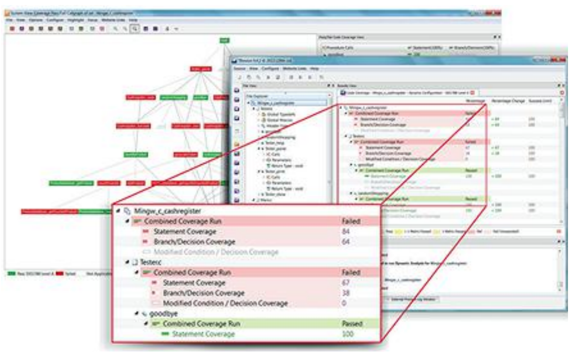
THE GPM-8213 digital power meter, designed by GW Instek specifically for single-phase (1P/2W) AC power supply's power measurements, includes a 4-in. TFT LCD, five-digit measurement display, 19 power measurement parameters, integral measurement function, front and rear panel input terminals, and various communications ports. Power measurement parameters include frequency, crest factor, apparent power, reactive power, power factor, phase angle, total harmonic distortion, and high-accuracy voltage, current and power measurement capabilities. TFT LCD advantages have been deployed to simple mode and standard mode. Simple mode displays conventional power meter's four measurement parameters to meet accuracy and clarity requirements for the test on manufacturing process. Standard mode extends the display to the maximum of 8 measurement parameters (2 major + 6 monitor measurements).

GW INSTEK, *www.gwinstek.com*

ARMv8-Based SBCs Built for High Performance Networking

THE NEWPORT FAMILY of SBCs from Gateworks includes eight standard models ranging in size and features for high performance embedded networking. Based upon the Cavium Octeon TX 64-bit ARMv8 SoC, the family offers processors ranging from an 800 MHz Dual Core up to a 1.5 GHz Quad Core. The boards feature up to 8 GB DDR4 DRAM, up to 64 GB eMMC Flash, up to five GbE Copper ports, up to two SFP ports, microSD, serial ports, GPIO, SPI/I2C, and up to 4 Mini-PCIe expansion sockets allowing support for peripherals including: Wi-Fi radios, cellular modems and mSATA drives. An 8 - 60 Vdc input power supply provides up to 15 W to Mini-PCIe sockets for high-power radios and up to 15 W to USB jacks. Power is applied through barrel jack or Ethernet jack with either 802.3at or Passive PoE.

GATEWORKS, *www.gateworks.com*



Tool Suite Clears Path to IEC 62304 Compliance

A NEW VARIANT of LDRA's tool suite is specifically tailored to aid IEC 62304 compliance and the faster development of safety- and security-critical medical device applications. The tool suite automates software quality analysis and testing while providing a traceable, auditable workflow from requirements through deployment for Class II and Class III medical devices. The suite offers a comprehensive set of automated tools for the safe development, deployment, and maintenance of medical device software. Bidirectional traceability connects functional, safety, and security requirements to the objectives of IEC 62304 standard as well as the design, coding, and testing activities and artifacts. In addition to achieving compliance, the suite automates software test activities such as: software quality analysis; coding standard support for CERT, CWE, MISRA, company-defined and others; automated test case generation, test harness generation and test execution; and requirement change impact analysis and regression testing. The LDRA tool suite for Medical Devices will be available Q4 of 2017.

LDRA, *http://ldra.com*

Sensor Boosts NIR Image Quality in Surveillance Cameras

THE OS05A20 is OmniVision's first image sensor to implement its Nyxel NIR technology. The 5-megapixel color image sensor leverages both PureCel pixel architecture and Nyxel technology to capture bright, crisp videos and images, day and night. With QE improved to 850 and 940 nm while maintaining high modulation transfer function, the sensor can "see" better and farther under low- and no-light conditions, boosting image quality, extending image-detection range, and reducing the light-source requirement which leads to lower power consumption and the ability to provide covert surveillance. By combining the Nyxel technology with a 2 x 2 micron pixel format, the OS05A20 PureCel image sensor can capture high-quality, high-resolution day or night, targeting it for professional surveillance systems. Available in a 1/2.7-inch optical format, the component is capable of capturing full-resolution 2688 × 1944 video at 60 fps, 1080p full HD video at 120 fps, and 720p HD video at 180 fps. The OS05A20 PureCel image sensor comes in a 6.6 x 5.9 mm CSP.

OMNIVISION, *www.ovt.com*

INDEX

For more information on products or services visit our website **www.electronicdesign.com**, menu item Reader Service. The advertisers index is prepared as an extra service. *Electronic Design* does not assume any liability for omissions or errors.

MARIA GUERRA | Technology Editor
maria.guerra@penton.com

When Race-Car Drivers and Analysts Mingle

Emerging technologies from industries spanning the electronics spectrum hold court at the IDTechEx show.

The "car of the future" is almost here, and IDTechEx brought that concept to life via presentations given by powerhouses of industry ranging from the automotive arena to government and technology. Among the speakers were Julia Landauer, a two-time championship-winning NASCAR driver, who gave the keynote address.

Landauer hypothesized how auto racing and Silicon Valley, in conjunction with the auto industry, can learn from each other. Topics such as alternative energy sources, wearables (monitoring driver vitals), augmented reality (AR), and electric vehicles were covered in her address.

In addition, Dr. Carl Dietrick, CTO of Terrafugia, discussed the company's flying/driving vehicles (*see figure*), including some of its innovations in sensing, the Internet of Things (IoT), and autonomous systems.

Also on hand were a host of major car manufacturers, as well as representatives from various arms of government. For example, Porsche discussed technology in auto racing with e-mobility technical system engineer Ken Gould, focusing in on the relationship between motorsport activities, technical innovation, durability, and refinement.

With a session titled "Future electric vehicle adoption in California," the California Energy Commission delved into the development and implementation of electric-vehicle programs. In an autonomous vehicles session from Elix Wireless, Dr. Brice Jamieson, director of technology, discussed autonomous vehicles and the need for an autonomous charging solution.

Acknowledging the momentum behind energy-storage systems (ESS), Google gave a presentation on the overall market, technology advances, and cost of vanadium flow batteries for ESS. Mercedes-Benz Energy also is focused on this topic—Candice Yu, who's in charge of Policy and Strategic Planning at the company, offered her take on how automakers are driving energy storage adoption.

Additional presentations tackled subject matter such as new graphene and supercapacitor technologies that should even benefit IoT applications. There was also a conversation on hybrid vehicles led by Protean Electric, a company that designs, develops, and manufactures in-wheel motor solutions.

For more in-depth coverage of IDTechEx, visit *www.electronicdesign.com*.

Illustrating the increasing synergies between the electronics and automotive industries, Julia Landauer, a two-time championship-winning NASCAR driver, gave the keynote address at the recent IDTechEx show.

Optical Switch
Optimum Price

DTI'S NEW HIGH VOLTAGE OPTICAL SWITCH

For some time, Dean Technology has been providing custom solutions to customers using optical diode technology. We are now moving to make these custom products a part of our standard product offering, starting with a 10 kV optical switch / optocoupler, the OPC10M.

This first optical device from DTI consists of a central diode with two LED drivers allowing for variable high voltage output from a low voltage reference input. It is exceptionally space efficient, and the tight control of production methods will allow DTI to offer these parts at prices far better than competitive solutions.

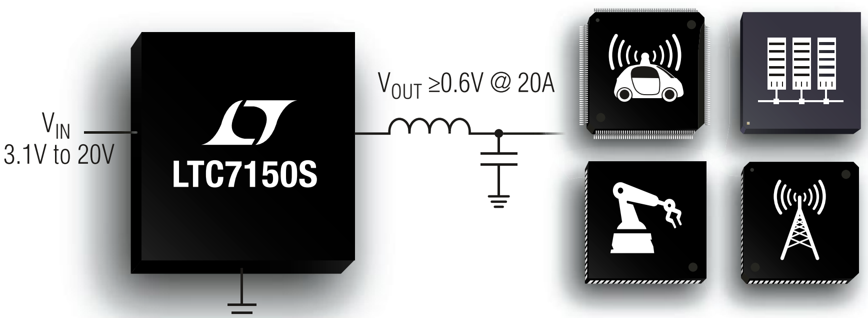
IN STOCK TODAY! Contact us for a quote or to place your order!

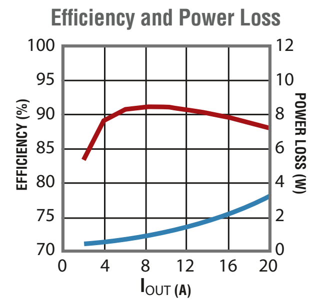
www.deantechnology.com

HVCA CKE HVPSI

Products By: DEAN TECHNOLOGY

$20V_{IN}$ & $20A_{OUT}$ Silent Switcher® 2





$12V_{IN}$ to $1.2V_{OUT}$, 92% Efficient Monolithic Buck

Need a high performance, high power point-of-load power supply for your digital IC (FPGA, uP, uC, DSP, GPU, PLD, ASIC)? The LTC7150S is a 20A, high efficiency monolithic synchronous buck regulator that incorporates Silent Switcher 2 technology, delivering excellent EMI performance while easing board layout. Its phase-lockable controlled on-time current mode architecture enables large step-down ratios at high switching frequencies to deliver high power density solutions. PolyPhase operation allows multiple LTC7150S regulators to run in parallel out-of-phase, reducing the amount of required input and output capacitance. Its operating supply voltage range is 3.1V to 20V, with an output voltage range of 0.6V to V_{IN}. With an operating frequency programmable from 400kHz to 3MHz, it can use physically smaller inductor and capacitor sizes, and can be externally synchronized over the same range for noise sensitive applications.

Selected Monolithic Single & Dual Buck Regulators

Part Number	I_{OUT}	V_{IN} Range	V_{OUT} Range	Freq (Max)	Differential Remote Sense	Silent Switcher	Package
LTC7150S	20A	3.1V to 20V	0.6V to V_{IN}	3MHz	Yes	SS 2 ^^	5 x 6 x 1.3mm BGA
LTC7151S*	15A	3.1V to 20V	0.5V to V_{IN}	3MHz	Yes	SS 2 ^^	4 x 5 x 0.75mm LQFN
LT8642S*	10A	3V to 18V	0.6V to V_{IN}	3MHz	No	SS 2 ^^	4 x 4 x 0.94mm LQFN
LT8652S*	8.5A/8.5A	3V to 18V	0.6V to V_{IN}	3MHz	Yes	SS 2 ^^	4 x 7 x 0.94mm LQFN
LTC3636	6A/6A	3.1V to 20V	0.6V to 12V	4MHz	No	No	4 x 5 x 0.75mm QFN
LTC7124	3.5A/3.5A	3.1V to 17V	0.6V to V_{IN}	4MHz	No	No	3 x 5 x 0.75mm QFN

** Future product, please contact for more information. ^^ SS 2 = noise-cancelling hot loops and integrated capacitors*

Info & Free Samples

www.linear.com/product/LTC7150S

1-800-4-LINEAR

LINEAR TECHNOLOGY | NOW PART OF ANALOG DEVICES

Find your local sales office: **www.linear.com/contact**